

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-196585

(43)Date of publication of application : 14.07.2000

(51)Int.Cl.

H04L 9/14
G11B 19/02
G11B 19/04
G11B 20/10

(21)Application number : 11-287365

(71)Applicant : MATSUSHITA ELECTRIC IND CO
LTD

(22)Date of filing : 07.10.1999

(72)Inventor : TAGAWA KENJI
MINAMI MASANAO
KOZUKA MASAYUKI
AOYAMA SHOICHI
TOKUDA KATSUMI
HIRATA NOBORU

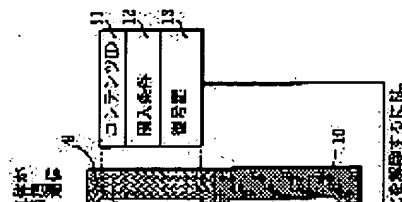
(30)Priority

Priority number : 10286177	Priority date : 08.10.1998	Priority country : JP
10297159	19.10.1998	
10297142	19.10.1998	JP
		JP

(54) RECORDING MEDIUM RECORDING CONTENTS, DIGITAL DATA RECORDER, DIGITAL DATA REPRODUCER, CONTENTS PACKAGING DEVICE GENERATING PACKAGE, CONTENTS REPRODUCER, COMPUTER READABLE RECORDING MEDIUM, RECORDING METHOD, REPRODUCING METHOD, PACKAGING METHOD AND SYSTEM TRANSPORT STREAM PROCESSOR CONSISTING OF CONTENTS PACKAGING DEVICE AND CONTENTS REPRODUCER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a recording medium by which, to a consumer having purchased



music contents, music contents relating to the music contents one sold at low cost and readily even when an infrastructure to realize electronic music distribution is not arranged.

SOLUTION: A recording medium records contents of purpose of sale and also records super distribution contents 10 that are encrypted on the basis of the block encryption method. A super distribution header 9 given to the super distribution contents 10 is encrypted on the basis of the encryption method that is an application of a public key and includes a decoding key 13 to decode the encryption of the block encryption method. In the case that the recording medium is loaded to a device connected to a communication channel, the encryption method that is an application of the public key can be decoded by the device and the decoding of the encryption is attended with charging through the communication channel.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号
特開2000-196585
(P2000-196585A)

(43)公開日 平成12年7月14日(2000.7.14)

(51)Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 L 9/14		H 0 4 L 9/00	6 4 1
G 1 1 B 19/02	5 0 1	C 1 1 B 19/02	5 0 1 J
19/04	5 0 1	19/04	5 0 1 H
20/10		20/10	H

審査請求 未請求 請求項の数29 O L (全 29 頁)

(21)出願番号	特願平11-287365	(71)出願人	000003821 松下電器産業株式会社 大阪府門真市大字門真1006番地
(22)出願日	平成11年10月7日(1999.10.7)	(72)発明者	田川 健二 大阪府門真市大字門真1006番地 松下電器産業株式会社内
(31)優先権主張番号	特願平10-286177	(72)発明者	南 賢尚 大阪府門真市大字門真1006番地 松下電器産業株式会社内
(32)優先日	平成10年10月8日(1998.10.8)	(74)代理人	100090446 弁理士 中島 司朗 (外1名)
(33)優先権主張国	日本 (J P)		
(31)優先権主張番号	特願平10-297159		
(32)優先日	平成10年10月19日(1998.10.19)		
(33)優先権主張国	日本 (J P)		
(31)優先権主張番号	特願平10-297142		
(32)優先日	平成10年10月19日(1998.10.19)		
(33)優先権主張国	日本 (J P)		

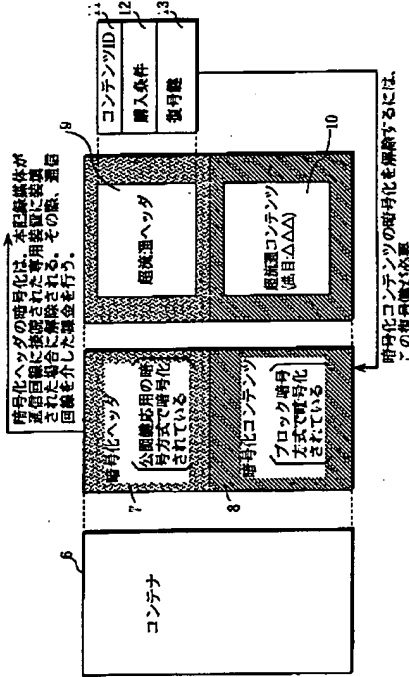
最終頁に続く

(54)【発明の名称】 コンテンツを記録した記録媒体、デジタルデータ記録装置、デジタルデータ再生装置、パッケージを作成するコンテンツパッケージング装置、コンテンツ再生装置、コンピュータ読み取り可能

(57)【要約】

【課題】 電子音楽配信を実現するためのインフラストラクチャが未整備であっても、ある音楽コンテンツを購入した消費者に対して、この音楽コンテンツに関連する音楽コンテンツを低価格で尚且つ手軽に販売することができる記録媒体を提供する。

【解決手段】 記録媒体には、販売目的のコンテンツが記録されており、それと共に、ブロック暗号方式に基づいて暗号化されている超流通コンテンツ10が記録されている。この超流通コンテンツ10に付与されている超流通ヘッダ9は、公開鍵応用の暗号化方式に基づいて暗号化されており、ブロック暗号方式の暗号化を解除させる復号鍵13を含む。この公開鍵応用の暗号化方式は、本記録媒体が通信回線に接続された装置300、400に装填された場合に、これらの装置により暗号化が解除される暗号方式であり、その暗号化の解除には、通信回線を介した課金が伴う。



(2) 000-196585 (P2000-196585A)

【特許請求の範囲】

【請求項1】 第1コンテンツと、

第1コンテンツとは異なるコンテンツであって、第1暗号方式に基づいて暗号化されている第2コンテンツと、第2コンテンツに対応づけられていて、第2コンテンツにおける暗号化を解除させるために用いられる第1鍵情報を含んでおり、所定の装置に予め配布されている第2鍵情報を用いた場合のみ、その暗号化の解除が行われる暗号方式である第2暗号方式にて暗号化されているヘッダとが記録されていることを特徴とする記録媒体。

【請求項2】 前記所定装置は、課金を行う機能を有しており、

前記ヘッダは更に、

第2コンテンツの再生又は他の記録媒体への記録を許諾するか否かと、再生又は他の記録媒体への記録を許諾する場合の上限回数とを示す利用制限情報と、

第2コンテンツの再生又は他の記録媒体に記録が許諾されている場合に、前記所定装置に課金させるべき再生に要する料金又は他の記録媒体への記録に要する料金を示す課金情報とを含むことを特徴とする請求項1記載の記録媒体。

【請求項3】 前記所定装置は、課金を行う機能を有しており、

前記ヘッダは更に、

第2コンテンツの再生又は他の記録媒体への記録を許諾するか否かと、再生又は他の記録媒体に記録を許諾する場合の許可期間を示す許可期間情報と、

第2コンテンツの再生又は他の記録媒体に記録が許諾されている場合に、前記所定装置に課金させるべき再生に要する料金又は他の記録媒体への記録に要する料金を示す課金情報とを含むことを特徴とする請求項1記載の記録媒体。

【請求項4】 前記第1コンテンツは、記録媒体固有の識別情報を用いて、暗号化されていることを特徴とする請求項1記載の記録媒体。

【請求項5】 コンテンツを含むデジタルデータを記録媒体に記録するデジタルデータ記録装置であって、記録媒体に記録すべきコンテンツを少なくとも1つ以上格納する格納手段と、

その再生又は他の記録媒体への記録に課金を行うべきものが前記1つ以上のコンテンツに存在する場合、そのコンテンツを超流通コンテンツとして選択する選択手段と、

課金が行われていない間、選択された超流通コンテンツについての再生又は他の記録媒体への記録を防止するよう、第1暗号方式に基づいて超流通コンテンツを暗号化する第1暗号化手段と、

超流通コンテンツの暗号化を解除させる鍵情報を含む超流通ヘッダを生成する生成手段と、

生成された超流通ヘッダを、前記第1暗号方式より安全

性が高い第2暗号方式に基づいて暗号化して、超流通コンテンツに付与する第2暗号化手段と、

超流通ヘッダが付与されると、1つ以上のコンテンツをデジタルデータとして記録媒体に記録する記録手段とを備えることを特徴とするデジタルデータ記録装置。

【請求項6】 前記デジタルデータ記録装置は更に記録媒体固有の識別情報を記録媒体から取り出す取出手段と、

超流通コンテンツ以外のコンテンツについては、取出手段により取り出された識別情報を用いて暗号化する第3暗号化手段とを備えることを特徴とする請求項5記載のデジタルデータ記録装置。

【請求項7】 他の記録媒体への記録に課金が必要であり、課金が行われていない間に他の記録媒体に記録されることを防止するため暗号化されているコンテンツである超流通コンテンツを第1記録媒体から読み出して、第2記録媒体に記録するデジタルデータ記録装置であって、

第1記録媒体及び第2記録媒体の少なくとも一方を装填する装填手段と、

装填手段に装填された記録媒体が第1記録媒体であれば、超流通コンテンツを第1記録媒体から読み出す読出手段と、

超流通コンテンツの第2記録媒体への記録に対する対価を操作者に提示する提示手段と、

操作者からの操作を受け付ける受付手段と、

受付手段が受け付けた操作が、対価の支払いに同意する旨の操作である場合、第1記録媒体から読み出された超流通コンテンツの暗号化を解除する解除手段と、

対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金手段と、

装填手段に超流通コンテンツの記録先となる第2記録媒体が装填されれば、暗号化が解除された超流通コンテンツをデジタルデータとして記録先の第2記録媒体に記録する記録手段とを備えることを特徴とするデジタルデータ記録装置。

【請求項8】 前記デジタルデータ記録装置は更に装填手段に超流通コンテンツの記録先となる第2記録媒体が装填されれば、記録媒体固有の識別情報を、記録先となる第2記録媒体から取り出す取出手段と、

解除手段により暗号化が解除された超流通コンテンツを、取出手段が取り出した識別情報を暗号鍵として用いて、再度暗号化する再暗号化手段とを備え、

前記記録手段は、

再暗号化手段により再度暗号化された超流通コンテンツを記録先の第2記録媒体に記録することを特徴とする請求項7記載のデジタルデータ記録装置。

【請求項9】 その再生に課金が必要であり、課金が行われていない間の再生を防止するため暗号化されているコンテンツである超流通コンテンツを再生するデジタル

(3) 000-196585 (P2000-196585A)

データ再生装置であって、
記録媒体を装填する装填手段と、
装填手段に装填された記録媒体に超流通コンテンツが記録されていればこれを読み出す読出手段と、
超流通コンテンツの再生に対する対価を操作者に提示する提示手段と、
操作者からの操作を受け付ける受付手段と、
受付手段が受け付けた操作が、対価の支払いに同意する旨の操作である場合、超流通コンテンツの暗号化を解除する解除手段と、
対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金手段と、
暗号化が解除された超流通コンテンツを再生する再生手段とを備えることを特徴とするデジタルデータ再生装置。

【請求項10】 複数のコンテンツを含むパッケージを作成するコンテンツパッケージング装置であって、
配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る符号化手段と、
再生品質の高低に応じて、各コンテンツをランク付けするランク付け手段と、
複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納する対応表格納手段と、
ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化手段と、
前記暗号化された複数のコンテンツを含むパッケージを生成する梱包手段とを備えることを特徴とするコンテンツパッケージング装置。

【請求項11】 前記対応表格納手段は、
前記高い品質で再生されるコンテンツには安全性が高い暗号が用いられるように、前記ランク情報と暗号鍵および暗号アルゴリズムを組にして格納していることを特徴とする請求項10記載のコンテンツパッケージング装置。

【請求項12】 複数のコンテンツを含むパッケージを作成するコンテンツパッケージング装置であって、
配布対象の一部分を符号化することにより試供用コンテンツを得ると共に、配布対象の残りの部分を符号化することにより差分コンテンツを得る符号化手段と、
試供用コンテンツに所定のランクを付与し、差分コンテンツに、より高いランクを付与するランク付け手段と、
複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にしており、一方の組には、所定のランクが対応づけられ、他方の組には、当該所定のランクより高いランクに対応づけられている対応表を格納している対応表格納手段と、
ランクが付与されたコンテンツを、対応表に示されてい

るランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化手段と、

前記暗号化された複数のコンテンツを含むパッケージを生成する梱包手段とを備えることを特徴とするコンテンツパッケージング装置。

【請求項13】 パッケージからコンテンツを取り出して再生するコンテンツ再生装置であって、
再生装置のハードウェアの性能を評価して、当該ハードウェアの性能を示すランク値を算出する評価手段と、
複数のランク値と、各ランク値に対応する性能を有するハードウェアが暗号化解除処理を行う際、その暗号化解除処理に用いるべき復号鍵及び復号アルゴリズムの組みとを対応づけた対応表を格納している対応表格納手段と、
それぞれが暗号化がなされたコンテンツを複数含むパッケージを装置外部から取得する取得手段と、
対応表における複数の復号鍵及び復号アルゴリズムのうち、評価手段により評価されたランク値に応じたものを選択すると共に、この復号鍵及び復号アルゴリズムにて暗号化が解除されるべきコンテンツをパッケージから取り出して、取り出されたコンテンツの暗号化を解除する解除手段とを備えることを特徴とするコンテンツ再生装置。

【請求項14】 配布対象の一部分を符号化することにより得られた試供用コンテンツと、配布対象の残りの部分を符号化して、試供用コンテンツより安全性が高い暗号鍵及び暗号アルゴリズムにて暗号化することにより得られた差分コンテンツとを含むパッケージからコンテンツを取り出して再生するコンテンツ再生装置であって、
再生装置のハードウェアの性能を評価して、当該ハードウェアの性能を示すランク値を算出する評価手段と、
試供用コンテンツの暗号化を解除することができる復号鍵及び復号アルゴリズムを低いランク値と対応づけており、差分コンテンツの暗号化を解除することができる復号鍵及び復号アルゴリズムを高いランク値と対応づけた対応表を格納している対応表格納手段と、
それぞれが暗号化がなされたコンテンツを複数含むパッケージを装置外部から取得する取得手段と、
対応表における複数の復号鍵及び復号アルゴリズムのうち、評価手段により評価されたランク値に対応したものを選択すると共に、取得したパッケージから、試供用コンテンツ及び差分コンテンツの何れか一方を取り出して、取り出されたコンテンツの暗号化を解除する解除手段とを備えることを特徴とするコンテンツ再生装置。

【請求項15】 所定の暗号鍵及び所定の暗号化アルゴリズムにて暗号化された試供用コンテンツと、
試供用コンテンツより高い品質で再生され、前記所定の暗号鍵及び前記所定の暗号化アルゴリズムより安全性がより高い暗号鍵及び暗号化アルゴリズムにて暗号化された販売用コンテンツとが記録されていることを特徴とす

(4) 000-196585 (P2000-196585A)

る記録媒体。

【請求項16】 配布対象の一部分を符号化した後、所定の暗号鍵及び所定の暗号化アルゴリズムにて暗号化することにより得られた試供用コンテンツと、配布対象の残りの部分を符号化した後、前記所定の暗号鍵及び前記所定の暗号化アルゴリズムより安全性がより高い暗号鍵及び暗号化アルゴリズムにて暗号化することにより差分コンテンツとが記録されていることを特徴とする記録媒体。

【請求項17】 複数のコンテンツを含むパッケージを作成するコンテンツパッケージング装置と、パッケージからコンテンツを取り出して再生するコンテンツ再生装置とからなるシステムであって、

前記コンテンツパッケージング装置は、

配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る符号化手段と、再生品質の高低に応じて、各コンテンツをランク付けするランク付け手段と、

複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納しており、一方の組には、所定のランクが対応づけられ、他方の組には、当該所定のランクより高いランクに対応づけられている対応表を格納する第1対応表格納手段と、

ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化手段と、

前記暗号化された複数のコンテンツを含むパッケージを生成する梱包手段とを備え、

前記コンテンツ再生装置は、

再生装置のハードウェアの性能を評価して、当該ハードウェアの性能を示すランク値を算出する評価手段と、

複数のランク値と、各ランク値に対応する性能を有するハードウェアが暗号化解除処理を行う際、その暗号化解除処理に用いるべき復号鍵及び復号アルゴリズムとを対応づけた対応表を格納している第2対応表格納手段と、それぞれが暗号化がなされたコンテンツを複数含むパッケージを装置外部から取得する取得手段と、

対応表における複数の復号鍵及び復号アルゴリズムのうち、評価手段により評価されたランク値に応じたものを選択すると共に、この復号鍵及び復号アルゴリズムにて暗号化が解除されるべきコンテンツをパッケージから取り出して、取り出されたコンテンツの暗号化を解除する解除手段とを備えることを特徴とするシステム。

【請求項18】 コンテンツを少なくとも1つ以上格納する格納部を有したコンピュータが、読み取ることができる記録媒体であって、

その再生又は他の記録媒体への記録に課金を行うべきものが前記1つ以上のコンテンツに存在する場合、そのコンテンツを超流通コンテンツとして選択する選択ステッ

プと、

課金が行われていない間、選択された超流通コンテンツについての再生又は他の記録媒体への記録を防止するよう、第1暗号方式に基づいて超流通コンテンツを暗号化する第1暗号化ステップと、

超流通コンテンツの暗号化を解除させる鍵情報を含む超流通ヘッダを生成する生成ステップと、

生成された超流通ヘッダを、前記第1暗号方式より安全性が高い第2暗号方式に基づいて暗号化して、超流通コンテンツに付与する第2暗号化ステップと、超流通ヘッダが付与されると、1つ以上のコンテンツをデジタルデータとして記録媒体に記録する記録ステップとからなる手順をコンピュータに行わせる記録プログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項19】 第1記録媒体、及び、第2記録媒体の何れか一方を装填する装填部を有したコンピュータが読み取ることができる記録媒体であって、

課金が行われていない間に他の記録媒体に記録されることを防止するため暗号化されている超流通コンテンツが記録された第1記録媒体が、装填部に装填されればこれを第1記録媒体から読み出す読出ステップと、

超流通コンテンツの第2記録媒体への記録に対する対価を操作者に提示する提示ステップと、

操作者からの操作を受け付ける受付ステップと、

受付ステップが受け付けた操作が、対価の支払いに同意する旨の操作である場合、第1記録媒体から読み出された超流通コンテンツの暗号化を解除する解除ステップと、

対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金ステップと、

装填部に超流通コンテンツの記録先となる第2記録媒体が装填されれば、暗号化が解除された超流通コンテンツをデジタルデータとして記録先の第2記録媒体に記録する記録ステップとからなる手順をコンピュータに行わせる記録プログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項20】 記録媒体を装填する装填部を有したコンピュータが読み取ることができる記録媒体であって、その再生に課金が必要であり、課金が行われていない間の再生を防止するため暗号化されている超流通コンテンツが記録された記録媒体が装填部に装填されれば、超流通コンテンツを読み出す読出ステップと、

超流通コンテンツの再生に対する対価を操作者に提示する提示ステップと、操作者からの操作を受け付ける受付ステップと、

受付ステップが受け付けた操作が、対価の支払いに同意する旨の操作である場合、超流通コンテンツの暗号化を解除する解除ステップと、

対価の支払いに同意する旨の指示を操作者から受け付け

(5) 000-196585 (P2000-196585A)

た場合、操作者に対して課金を行う課金ステップと、操作者に対して課金が行われると、暗号化が解除された超流通コンテンツを再生する再生ステップとからなる手順をコンピュータに行わせる再生プログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項21】 複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納している対応表格納部を有したコンピュータが読み取ることができる記録媒体であって、

配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る符号化ステップと、

再生品質の高低に応じて、各コンテンツをランク付けするランク付けステップと、

ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化ステップと、

前記暗号化された複数のコンテンツを含むパッケージを生成する梱包ステップとからなる手順をコンピュータに行わせるパッケージングプログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項22】 複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納する格納部を有したコンピュータが読み取ることができる記録媒体であって、配布対象の一部分を符号化することにより試供用コンテンツを得ると共に、配布対象の残りの部分を符号化することにより差分コンテンツを得る前記符号化ステップと、

試供用コンテンツに所定のランクを付与し、差分コンテンツに、より高いランクを付与するランク付けステップと、

ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化ステップと、

前記暗号化された複数のコンテンツを含むパッケージを生成する梱包ステップとからなる手順をコンピュータに行わせるパッケージングプログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項23】 複数のランク値と、各ランク値に対応する性能を有するハードウェアが暗号化解除処理を行う際、その暗号化解除処理に用いるべき復号鍵及び復号アルゴリズムとを対応づけた対応表を格納している格納部を有するコンピュータが読み取ることができる記録媒体であって、

コンピュータのハードウェアの性能を評価して、当該ハードウェアの性能を示すランク値を算出する評価ステップと、

それぞれが暗号化がなされたコンテンツを複数含むパッケージをコンピュータ外部から取得する取得ステップと、

対応表における複数の復号鍵及び復号アルゴリズムのうち、評価ステップにより評価されたランク値に応じたものを選択すると共に、この復号鍵及び復号アルゴリズムにて暗号化が解除されるべきコンテンツをパッケージから取り出して、取り出されたコンテンツの暗号化を解除する解除ステップとからなる手順をコンピュータに行わせるパッケージングプログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項24】 記録媒体に記録すべきコンテンツを少なくとも1つ以上格納する格納部を有したコンピュータが、コンテンツを含むデジタルデータを記録媒体に記録する記録方法であって、

その再生又は他の記録媒体への記録に課金を行うべきものが前記1つ以上のコンテンツに存在する場合、そのコンテンツを超流通コンテンツとして選択する選択ステップと、

課金が行われていない間、選択された超流通コンテンツについての再生又は他の記録媒体への記録を防止するよう、第1暗号方式に基づいて超流通コンテンツを暗号化する第1暗号化ステップと、

超流通コンテンツの暗号化を解除させる鍵情報を含む超流通ヘッダを生成する生成ステップと、

生成された超流通ヘッダを、前記第1暗号方式より安全性が高い第2暗号方式に基づいて暗号化して、超流通コンテンツに付与する第2暗号化ステップと、超流通ヘッダが付与されると、1つ以上のコンテンツをデジタルデータとして記録媒体に記録する記録ステップとからなる手順をコンピュータに行わせることを特徴とする記録方法。

【請求項25】 前記記録方法は、第1記録媒体及び第2記録媒体の何れかを装填する装填部を有したコンピュータに適用され、第1記録媒体に記録された超流通コンテンツを含むデジタルデータを第2記録媒体に記録する記録方法であって、第2記録媒体への記録に課金が必要であり、課金が行われていない間に第2記録媒体に記録されることを防止するため暗号化されている超流通コンテンツが記録された第1記録媒体が装填部に装填されればこれを第1記録媒体から読み出す読出ステップと、超流通コンテンツの第2記録媒体への記録に対する対価を操作者に提示する提示ステップと、

操作者からの操作を受け付ける受付ステップと、受付ステップが受け付けた操作が、対価の支払いに同意する旨の操作である場合、第1記録媒体から読み出された超流通コンテンツの暗号化を解除する解除ステップと、

対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金ステップと、

(6) 000-196585 (P2000-196585A)

装填部に超流通コンテンツの記録先となる第2記録媒体が装填されれば、暗号化が解除された超流通コンテンツをデジタルデータとして記録先の第2記録媒体に記録する記録手段とからなる手順をコンピュータに行わせることを特徴とする記録方法。

【請求項26】 記録媒体を装填する装填部を有したコンピュータに適用され、記録媒体に記録されているデジタルデータを再生する再生方法であって、装填部に装填された記録媒体に、その再生に課金が必要であり、課金が行われていない間の再生を防止するため暗号化されている超流通コンテンツが記録されているばこれを読み出す読出ステップと、超流通コンテンツの再生に対する対価を操作者に提示する提示ステップと、操作者からの操作を受け付ける受付ステップと、受付ステップが受け付けた操作が、対価の支払いに同意する旨の操作である場合、超流通コンテンツの暗号化を解除する解除ステップと、対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金ステップと、操作者に対して課金が行われると、暗号化が解除された超流通コンテンツを再する再生ステップとからなる手順をコンピュータに行わせることを特徴とする再生方法。

【請求項27】 複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納している対応表格納部を有したコンピュータに適用され、複数のコンテンツを含むパッケージを作成するコンテンツパッケージング方法であって、配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る符号化ステップと、再生品質の高低に応じて、各コンテンツをランク付けするランク付けステップと、ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化ステップと、前記暗号化された複数のコンテンツを含むパッケージを生成する梱包ステップとからなる手順をコンピュータに行わせることを特徴とするコンテンツパッケージング方法。

【請求項28】 複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納する格納部を有したコンピュータに適用され、複数のコンテンツを含むパッケージを作成するコンテンツパッケージング方法であって、配布対象の一部分を符号化することにより試供用コンテンツを得ると共に、配布対象の残りの部分を符号化することにより差分コンテンツを得る前記符号化ステップ

と、試供用コンテンツに所定のランクを付与し、差分コンテンツに、より高いランクを付与するランク付けステップと、ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化ステップと、前記暗号化された複数のコンテンツを含むパッケージを生成する梱包ステップとからなる手順をコンピュータに行わせることを特徴とするコンテンツパッケージング方法。

【請求項29】 複数のランク値と、各ランク値に対応する性能を有するハードウェアが暗号化解除処理を行う際、その暗号化解除処理に用いるべき復号鍵及び復号アルゴリズムとを対応づけた対応表を格納部を有したコンピュータに適用され、パッケージからコンテンツを取り出して再生するコンテンツ再生方法であって、コンピュータのハードウェアの性能を評価して、当該ハードウェアの性能を示すランク値を算出する評価ステップと、それぞれが暗号化がなされたコンテンツを複数含むパッケージをコンピュータ外部から取得する取得ステップと、対応表における複数の復号鍵及び復号アルゴリズムのうち、評価ステップにより評価されたランク値に応じたものを選択すると共に、この復号鍵及び復号アルゴリズムにて暗号化が解除されるべきコンテンツをパッケージから取り出して、取り出されたコンテンツの暗号化を解除する解除ステップとからなる手順をコンピュータに行わせることを特徴とする再生方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタル化された音楽著作物を初めとするコンテンツを記録した記録媒体、コンテンツを記録媒体に記録する装置、記録媒体に記録されているコンテンツを再生する装置、複数のコンテンツをパッケージングする装置、コンピュータ読み取り可能な記録媒体、記録方法、再生方法、パッケージング方法に関する。

【0002】

【従来の技術】（第1従来技術）次世代の音楽著作物の販売形態がどうあるべきかが、大手音楽会社、音響機器メーカー、有識者の間で盛んに議論されている。現状の音楽著作物の販売形態とは、ポップス、ロック、クラシック等様々なジャンルの音楽著作物をCD、磁気テープ等の記録媒体に記録して販売するという形態であり、このように販売された記録媒体を購入して音楽著作物を鑑賞するというライフスタイルは世界中に浸透しているといえる。

【0003】記録媒体を用いた販売形態に対抗する販売

(7) 000-196585 (P2000-196585A)

形態として、多くの注目を集めているのは、電子音楽配信と呼ばれる販売形態である。電子音楽配信とは、音楽コンテンツ（コンテンツとは、デジタル化された著作物のことをいい、音楽コンテンツとは、特に、デジタル化された音楽著作物のことをいう）の有料配布を、近年、急速な普及を見せているインターネット上で行うものである。この電子音楽配信の特色は、音楽コンテンツの販売の申し出や、音楽コンテンツを購入した者に対しての課金が電子商取引（Electronic Commerce）に準じて行われる点である。即ち、この電子音楽配信において音楽会社は、自身が開設したホームページに様々なコンテンツを紹介しており、消費者は、各音楽会社のホームページをアクセスすることにより、様々なコンテンツを検索することができる。好みのコンテンツがあった場合、消費者はコンテンツの購入要求、操作者ID等を、この音楽会社に通知する。音楽会社は、予め操作者により通知されているクレジットカードの番号に対応する銀行口座に基づいて、コンテンツの購入代金の決済を行うことができる。このような決済後、消費者は、消費者が所有しているコンピュータにコンテンツをダウンロードし、自分の好みのコンテンツを入手することができる。

【0004】このように電子音楽配信では、対話的な選択操作に応じてダウンロードを行うので、例えば、認知度が高い新譜のコンテンツの販売を行っているホームページにおいて、その新譜のコンテンツを作詞作曲したアーティストの他の楽譜のコンテンツや、その新譜のコンテンツを歌う歌手の他の楽譜のコンテンツを紹介すれば、これら他の楽譜を消費者に売り込むことができる。即ち、あるアーティストの新譜を購入しようとする消費者は、そのアーティストの関連する楽譜に強い興味を示していることが統計的に明らかであり、電子音楽配信では、そのような関連する複数の楽譜の売り込みを効率的に行うことができるのである。

【0005】（第2従来技術）第1従来技術で述べたように、音楽コンテンツの配布形態には、記録媒体を用いた販売形態、インターネット等の通信回線を用いた販売形態を初め様々なものがある。記録媒体と一言でいっても、記録媒体には、DVD-Audio、CD等の種類があり、これらは何れも異なった符号化方式により符号化された状態で音楽コンテンツを記録している。また、このような販売形態以外にも、衛星放送やケーブルTV等の放送波にて放送されることにより音楽コンテンツが配布される機会も多い。これらの配布は有償で行われるのが原則であるが、音楽コンテンツの知名度を高める目的で無償で試供される場合もある。

【0006】記録媒体、放送波、通信回線というように、様々な形態で音楽著作物が配布される場合、たとえ配布すべき音楽著作物が一種類のみであっても、音楽著作物を配布する側は、それぞれの配布形態に応じた形態の音楽コンテンツを作成して配布せねばならない。ここ

で、異なる符号化方式で符号化せねばならないのは以下の理由による。即ち、既に各世帯に普及している再生装置、及び、これから普及しつつある再生装置には、著作権保護機構の有無や、暗号鍵の安全性の高低、再生時における音楽コンテンツの再生品質の高低が、再生装置毎に異なるので、音楽コンテンツを同一の符号化方式にて一律に送信しても、著作権保護機構が全く活用されなかったり、再生装置が本来備えている再生能力が発揮できない恐れがあるからである。

【0007】著作権保護機構が既に整備されている再生装置が存在するのなら、全ての形態で配布される音楽コンテンツを安全性が高い暗号鍵にて暗号化しておけば良いように思える。しかし音楽コンテンツには、試供用等、知名度向上の目的で配布されるものがあり、このような音楽コンテンツは低い品質で再生されれば良いので、そのように、低い品質でしか再生されない音楽コンテンツも一律に安全性が高い暗号鍵にて暗号化すれば、試供用に低い品質のコンテンツを再生するにも、そのような安全性が高い暗号鍵による暗号化を解かねばならない。これでは、安全性が高い暗号化を解除するだけの復号能力を有していない再生装置は、試供用のコンテンツを再生することが不可能となり、試供用コンテンツが再生される機会が少なくなってしまう。このように試供用コンテンツが再生される機会が少くなれば、音楽コンテンツの試供にて、幅広く販売促進を図るという広告活動が本来の目標を失うことになる。以上の理由で、それぞれの配布形態に応じた形態の音楽コンテンツを作成して配布することが、必然的に行われていた。

【0008】

【発明が解決しようとする課題】ところで第1従来技術において問題となるのは、電子音楽配信を実現するためのインフラストラクチャは、現状、充分整備されているとはいえず、消費者が電子音楽配信にて音楽コンテンツを入手するには、消費者に様々な負担が課されるという点である。ここで電子音楽配信の実現のために不可欠とされているインフラストラクチャのうち、代表的なものは、数メガバイトというデータサイズを有する音楽コンテンツを短時間で伝送することができる高速回線であるが、一般のインターネットユーザは、公衆回線を介してサーバをアクセスを行うことにより、インターネットを利用している。一般のインターネットユーザが利用する公衆回線の伝送速度は、高速回線の伝送速度を大きく下回ることが一般的である。このように一般のインターネットユーザが低速な公衆回線を介して、上述のように複数コンテンツを同時にダウンロードする場合、通信時間が長時間となるので、消費者は、多大な通信料金を通信会社に支払うことになる。極端な場合、コンテンツの購入に関し消費者が音楽会社に支払う料金よりも、通信料金のほうが高くなってしまふことが有り得る。このように、消費者に多大な料金が課されるのであれば、電子音

(8) 000-196585 (P2000-196585A)

楽配信を利用しようとする消費者の意欲は消沈してしまう。この料金面の問題にも増して懸念されるのは、複数のコンテンツを送信する場合、公衆回線における転送に要する時間が極めて長くなるので、コンテンツの購入を希望した者を悪戯に苛立たせてしまう点である。このようにコンテンツの転送が長ければ、コンテンツの購入を希望した者は複数コンテンツのダウンロードの途中で、コンテンツの購入をキャンセルしてしまう可能性がある。

【0009】かといって、記録媒体を用いた販売形態において、電子音楽配信と同様、関連する楽譜のコンテンツを売り込もうとする場合、記録媒体を収納したケースに同梱されるジャケットに、そのような関連する楽譜についてセールスポイントや、販売価格等を印刷しておく、関連楽譜の購入を推薦するという古典的な手法をとらざるを得ない。消費者は、このようなジャケットの印刷内容を見て、関連楽譜に興味を持った場合、その関連楽譜を購入するためコンテンツの小売り店に出向き、その関連楽譜が記録された記録媒体を購入することにより、関連楽譜を入手するのである。

【0010】ここで小売り店に販売されている記録媒体の小売り価格には、記録媒体の製造や流通に係る様々なコストが計上されている。そのため、新譜が記録された記録媒体、関連楽譜が記録された記録媒体の双方を購入しようとする場合、それら記録媒体の製造や流通に係る様々なコストが計上された小売り価格を、2つのコンテンツのそれぞれについて支払う必要があるため、割高な料金を消費者は支払うことになる。

【0011】また、現状の記録媒体を用いた販売形態において、消費者が関連楽譜を入手するには、消費者自身がわざわざ記録媒体の小売り店に出向かねばならないので、消費者は気軽に関連楽譜を購入することはできず、記録媒体の小売り店に出向くまでにそのような関連楽譜を購入しようとする意欲を失ってしまうこともある。また第2の従来技術において、音楽コンテンツの供給者は、配布形態に応じて、異なる符号化方式で符号化を行う必要があるため、符号化されるコンテンツの数が多ければ多い程、音楽コンテンツの供給者は、それら音楽コンテンツの管理及び配布に多大なストレスを感じるという点である。このようにストレスを感じるのは、符号化されるコンテンツの数が多くなれば、例えば、販売用のコンテンツと、試供用のコンテンツとを誤って配布する等、誤配布の確率も高くなるからである。このような誤配布が生じれば、販売用コンテンツが公共の場に流出することになり、それらの全てを回収せねば、音楽コンテンツの供給者は経済的に大打撃を被ることになる。

【0012】本発明の第1の目的は、電子音楽配信を実現するためのインフラストラクチャが未整備であっても、ある音楽コンテンツを購入した消費者に対して、この音楽コンテンツに関連する音楽コンテンツを低価格で

尚且つ手軽に販売することができる記録媒体を提供することである。本発明の第2の目的は、著作権保護機構の有無や、暗号鍵の安全性の高低、再生時における音楽コンテンツの再生品質の高低が、再生装置毎に異なる場合であっても、これらに対する音楽コンテンツの配信を一律に行うことができるコンテンツ梱包装置を提供することである。

【0013】

【課題を解決するための手段】上記第1の目的は、第1コンテンツと、第1コンテンツとは異なるコンテンツであって、第1暗号方式に基づいて暗号化されている第2コンテンツと、第2コンテンツに対応づけられていて、第2コンテンツにおける暗号化を解除させるために用いられる第1鍵情報を含んでおり、所定の装置に予め配布されている第2鍵情報を用いた場合のみ、その暗号化の解除が行われる暗号方式である第2暗号方式にて暗号化されているヘッダとが記録されている記録媒体により達成される。

【0014】第2の目的は、配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る符号化手段と、再生品質の高低に応じて、各コンテンツをランク付けするランク付け手段と、複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納する対応表格納手段と、ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化手段と、前記暗号化された複数のコンテンツを含むパッケージを生成する梱包手段とを備えるコンテンツパッケージング装置により達成される。

【0015】

【発明の実施の形態】本発明に係る記録媒体、再生装置、記録装置についての実施形態について説明する。尚、記録媒体、再生装置、記録装置を一つの実施形態で説明しようとするとは説明が著しく煩雑になるので、上記の内容を第1実施形態から第6実施形態において個別に説明するものとする。

【0016】(第1実施形態)第1実施形態では、音楽コンテンツの販売用途に用いられる記録媒体について説明する。音楽コンテンツの販売用途に用いられる記録媒体には、販売目的の音楽コンテンツが記録されており、この記録媒体が有償で譲渡されることにより、コンテンツの販売がなされる。このような販売用途の記録媒体には、2つのタイプがある。1つ目のタイプは、販売を目的とした音楽コンテンツをEnhanced-CDに記録したものである。Enhanced-CDとは、内周部が通常のCD(CD-DA)と同じ物理構造になっていて、外周部がCD-ROMと同じ物理構造になっておりCD、CD-ROMの両方の機能を兼備したディスクをいう。本Enhanced-CDの外観を図1(a)に示し、Enhanced-CDの物理構造を図1(b)に示す。図1

(9) 000-196585 (P2000-196585A)

(a)においてEnhanced-CDの内周部は、CD-DA部と呼ばれ、外周部は、CD-ROM部と呼ばれる。これら、CD-DA部と、CD-ROM部を機能的に考えると、CD-DA部は、音楽コンテンツ3が記録されているコンテンツ領域1であり、CD-ROM部は、本記録媒体の付加価値を高めるデータを記録した付加価値領域2である。この販売用記録媒体は、このコンテンツ領域1に記録された音楽コンテンツを販売する用途に用いられる。

【0017】2つ目のタイプの販売用途の記録媒体は、販売目的の音楽コンテンツ3が記録されたDVD-AUDIOである。本DVD-AUDIOの外観を図2(a)に示し、その論理フォーマットを図2(b)に示す。このDVD-AUDIOにはEnhanced-CDに示したCD-DA部と、CD-ROM部は存在しないのに対して、販売目的のコンテンツ3、再生制御スクリプト4、静止画データ5、コンテナ6のそれぞれがパーソナルコンピュータでアクセス可能なファイルにて記録される。このようにファイルにて記録される点がEnhanced-CDと異なるが、機能的なデータ構造はEnhanced-CD同様であり、コンテンツ領域1と、付加価値領域2とからなる。また、DVD-AUDIOにおけるコンテンツ領域1に音楽コンテンツ3が記録され、付加価値領域2に本記録媒体の付加価値を高めるデータが記録されている点も、Enhanced-CDと同一である。Enhanced-CDとの違いは、Enhanced-CDのコンテンツ領域1には、販売目的のコンテンツ3が何の暗号化も施されることなく、そのまま記録されているのに対して、DVD-AUDIOのコンテンツ領域1に記録されている販売目的の音楽コンテンツ3は、DVD-AUDIO固有の識別情報を用いて暗号化されている点である。

【0018】これらの2つのタイプの販売用記録媒体は、通常のCDと同様、ジャケットや譜面カードを同梱した状態で、専用のプラスチックケースに収納される。図3は、販売用記録媒体を収納した専用のプラスチックケースを示す図である。ここでコンテンツ領域1に記録されているコンテンツの曲名を仮に曲名:〇〇〇とすれば、販売用記録媒体のジャケットには、図3に示すように、曲名:〇〇〇に関する写真が主として印刷されていることがわかる。

【0019】以上の説明で、コンテンツ領域1、付加価値領域2はEnhanced-CD及びDVD-AUDIOの双方に存在することが明らかになった。続いて、付加価値領域2の記録内容について説明する。図1(b)及び図2(b)の右段に付加価値領域2の記録内容を示す。本図に示すように、付加価値領域2には、再生制御スクリプト4と、静止画データ5と、コンテナ6とが記録されていることがわかる。

【0020】再生制御スクリプト4は、表示機能付きの装置に本販売用記録媒体が装填された場合、この装置の対話画面に表示させる内容を記述した情報であり、Macromedia Director形式、HTML形式で記述されている。ここでMacromedia Director形式とは、MS-Windows/MacOS

の汎用オーサリングソフトの利用時にオーサリング手順の記述に用いられる形式であり、HTML形式とは、インターネットブラウザの記述に頻用されている形式である。

【0021】静止画データ5は、再生制御スクリプト4により再生される対話画面において、表示されるべき静止画像である。これらの再生制御スクリプト4、静止画データ5は、従来のEnhanced-CDにも存在するものであるが、本実施形態における静止画データ5及び再生制御スクリプト4は、従来のものと表示内容が異なる。即ち、従来の静止画データ5及び再生制御スクリプト4には、販売目的のコンテンツ3の歌詞やプロモーション映像、ファンクラブや新譜案内等、販売目的のコンテンツ3に関連する情報を表示させるものであるが、本実施形態における静止画データ5及び再生制御スクリプト4は、販売目的のコンテンツ3とは異なる音楽コンテンツの購入及び再生を推薦する情報を上記装置に表示させる。

【0022】例えば、販売目的のコンテンツ3がある人気アーティストの新譜ならば、本実施形態における再生制御スクリプト4は、その人気アーティストの過去のヒット曲の購入及び再生を推薦している。これら再生制御スクリプト4にて購入及び再生が推薦されている音楽コンテンツが何であるかは、以降の説明で明らかにしてゆく。

【0023】続いて、Enhanced-CD及びDVD-AUDIOの双方に含まれている付加価値領域2におけるコンテナ6について説明する。コンテナ6のデータ構造は、図4に示すものとなる。本図において、コンテナ6は、暗号化ヘッダ7と、暗号化コンテンツ8とからなり、暗号化ヘッダ7は超流通ヘッダ9を含んでいて、暗号化コンテンツ8は超流通コンテンツ10を含んでいる。

【0024】ここで“超流通”とは、筑波大学名誉教授森亮一氏らが唱えるデジタルコンテンツの流通形態である。超流通においてデジタルコンテンツは、予め定められた超流通ヘッダが付与された状態で流通する。この超流通ヘッダには、対価をうるべき権利者を示す対価の詳細に関する対価情報が記されており、消費者がこのデジタルコンテンツの利用を希望した場合、消費者が所有する機器がこれらの権利者情報 対価情報を解釈して使用記録を作成することにより、料金清算を行うのである。

【0025】超流通ヘッダ9、超流通コンテンツ10は、このような超流通を前提にした形式、即ち、超流通形式にて、コンテナ6内に収納されている。このように、コンテナ6内に暗号化された状態で収納されている超流通コンテンツ10こそ、静止画データ5及び再生制御スクリプト4にて、購入及び再生が推薦されている音楽コンテンツである。

【0026】上述したように超流通ヘッダ9には、権利者情報や対価情報等、超流通を安全に行うために重要な情報が示されているので、これの改竄等の不正行為を効率的に防止する必要がある。そのため、本実施形態にお

(00)00-196585 (P2000-196585A)

ける超流通ヘッダ9は、公開鍵暗号アルゴリズムを応用した暗号方式に基づいて暗号化されたデータ領域を含む（尚、超流通ヘッダ9全体が暗号化されていてもよい。以下の文では、超流通ヘッダ9全体が暗号化されているものとして説明を行う。）。一般に公開鍵暗号には、楕円暗号やRSA暗号(Rivest, Shamir, Adleman encryption)等の種類があることが広く知られている。これら公開鍵を用いて暗号化されたデータを復号するには、暗号化に用いた公開鍵とは異なる復号鍵を用いる必要があるので、公開鍵は、安全性が非常に高いといわれる。

【0027】しかしながら、本実施形態において超流通ヘッダ9を暗号化する際に用いられる公開鍵応用の暗号方式は、単に公開鍵を用いるだけではなく、以下の点が改良されている。即ち、本実施形態における公開鍵応用の暗号方式では、超流通ヘッダ9内のデータ領域の暗号化を解くための復号鍵が所定の専用装置に予め配布されており、販売用記録媒体がこの専用装置に装填された際に、超流通ヘッダ9の暗号化が解除されるのである。本実施形態においてこの専用装置は、通信回線に接続されており、超流通ヘッダ9の暗号化が解除され、超流通コンテンツが再生されようとする際、又は、超流通コンテンツが他の記録媒体に記録される際、超流通コンテンツについての権利者が正当な対価を得るよう、当該専用装置は、通信回線を介した課金を行うのである。尚、様々な超流通コンテンツを販売用記録媒体に記録させようとする場合、超流通コンテンツのそれぞれの超流通ヘッダについて、異なる公開鍵を用いる。一方、専用装置は、それらの超流通ヘッダが異なる公開鍵を用いて暗号化されていても、共通の復号鍵を用いてこの超流通ヘッダを復号する。また本実施形態において専用装置は、超流通コンテンツを再生又は買い取る際の課金を通信回線を介して行うものとして説明するが、課金情報をICカード等の別の記録媒体に記録しておき、課金情報についての決済を別の装置で行っても良い。また、別の装置にてプリペイドカードによる課金を行ってもよい。

【0028】超流通ヘッダ9の暗号化を解除するための復号鍵が専用装置に設けられており、販売用記録媒体上に存在しないので、悪意を持った者が販売用記録媒体を取得し、不正な機器を用いてこの超流通ヘッダ9の暗号化を解除しようとしたとしても、その暗号化が解除される確率は極めて低い。このように超流通コンテンツ10の暗号化を不法に解除するのは極めて困難なので、超流通コンテンツ10の商取引は、安全に行われる。

【0029】尚、超流通コンテンツ10の曲名を△△△とすると、図3に示すように、販売用記録媒体のジャケットには、△△△についての内容は一切印刷されていない。これは、一般の消費者が、「超流通コンテンツ10は販売目的コンテンツ3を購入した者に無償で供与されるのではないかと勘違いすることを防止するためである。

【0030】続いて、超流通ヘッダ9の内容について、図4を参照しながら説明する。図4において最も右側の段は、超流通ヘッダ9の内容を示している。ここからも理解できるように超流通ヘッダ9は、コンテンツID11、購入条件12、復号鍵13から構成されている。コンテンツID11は、超流通コンテンツ10を他のコンテンツと識別するための情報が記述されている。超流通コンテンツ10は音楽コンテンツであるので、ISRC(International Standard Recording Code)等の識別情報がコンテンツID11として記述される。ここでISRCとは、曲ごとにユニークに割り振られる固有のID情報であって、国コード(2つのASCII文字)、記録年(2桁の数字)、シリアル番号(5桁の数字)により構成される。

【0031】購入条件12は、コンテンツの購入条件に関する情報が記述されている。ここで、購入条件12の一例を図5に示す。図5において「再生許可回数」欄には、再生可能な上限値が整数で記述される。「デジタル出力許可回数」とは、専用装置にデジタル出力端子が備わっている場合、このデジタル出力端子を介したデジタル出力を許可するか否かを示し、許可する場合は、その出力回数が整数値で記述される。

【0032】「再生許可時間」欄は、コンテンツの再生を許可する時間、すなわち再生できる時間が記述される。「再生許可期日」欄は、コンテンツの再生を許可する期日が記述される。再生が許可された期日が過ぎた場合、そのコンテンツの再生はできないことになる。「課金情報」欄は、超流通コンテンツ10の買い取り時の価格、又は、再生時の価格を示す情報を含む。ここで、買い取り時の価格とは、コンテナ6内の超流通コンテンツ10を他の記録媒体に記録する際に操作者に課される価格をいい、再生時の価格とは、従量課金、即ち、コンテナ6内の超流通コンテンツ10の再生回数に応じた価格を表す。この課金情報は、電子商取引において、署名付きの購入申込書として扱われるものであり、これと、操作者IDとを専用装置が課金センタ内のホストコンピュータに送信することは、電子商取引において販売用記録媒体の所有者が超流通コンテンツ10の購入を申し込むことを意味する。即ち、記録媒体を装填した専用装置は、操作者が超流通コンテンツ10の再生又は買い取りに合意した場合、通信回線を介して、操作者IDと、この課金情報とを音楽会社の課金センタに送信する。一方、音楽会社の課金センタには、操作者の予めクレジットカード番号が登録されており、このカード番号に対応する銀行口座を予め知得しているので、操作者IDが送信されれば、その送信元の操作者のクレジットカード番号に対応する銀行口座から、課金情報に示される価格を引き落とすことにより、コンテンツの購入代金の決済を行う。

【0033】復号鍵13は、超流通コンテンツ10を復号するための復号鍵である。超流通コンテンツ10は、LPCM(Linear Pulse Code Modulation)形式、AAC(Adv

(註1) 00-196585 (P2000-196585A)

anced Audio Coding) 形式、DTS (Digital Theater System) 形式の音楽コンテンツであり、ブロック暗号方式で暗号化されている。ブロック暗号とは、コンテンツをある一定の長さ(ブロック長)毎に分割して、そのブロック単位で暗号化する方法のことをいい、DES(ブロック長は64bit固定)、RC5(ブロック長は可変)などがこれに相当する。このブロック暗号方式では、暗号化したキーと復号化するための鍵とが同一であるので、公開鍵暗号、安全性は高く無い。超流通コンテンツ10の暗号化を解除するには復号鍵13を手入れせねばならないが、復号鍵13は公開鍵暗号方式で強固に暗号化された超流通ヘッダ9内に存在するので、安全性が高く、超流通コンテンツ10の暗号化を不法に解除することは非常に困難である。結果として超流通コンテンツ10は強固に保護されていることになる。

【0034】このように、超流通コンテンツ10の購入等に関する購入条件12は、安全性が高い公開鍵にて暗号化されている超流通ヘッダ9内に含まれているので、課金情報の改竄や超流通ヘッダ9の復号は非常に困難となる。また、超流通コンテンツ10を公開鍵にて暗号化するのではなく、超流通ヘッダ9のみが公開鍵にて暗号化されているので、超流通コンテンツ10を得るには、超流通ヘッダ9の暗号化を解除して、復号鍵13を取り出し、復号鍵13を用いて超流通コンテンツ10を解除すればよい。公開鍵暗号方式で暗号化されている部分はヘッダ部分に限定されているので、暗号化を解除すべき箇所は短く、超流通コンテンツ10の買取や再生を指示してから、買取や再生が可能となる時間は短くて済むので、超流通コンテンツ10を希望した者を悪戯に苛立たせることはない。この解除に要する時間は、電子音楽配信における音楽コンテンツのダウンロードに要する時間より極めて短くなると考えられるので、操作者は、買取又は再生を希望した超流通コンテンツ10をすぐさま鑑賞することができる。

【0035】続いて、販売目的コンテンツ、超流通ヘッダ及び超流通コンテンツについての管理情報について説明する。ここで販売目的コンテンツは、CD、DVD-AUDIOにおける管理情報にて管理されているが、超流通ヘッダ及び超流通コンテンツは、そのような管理情報にて管理されていない。このように販売目的コンテンツは、CD、DVD-AUDIOにおける管理情報にて管理されているため、CDプレーヤ、DVD-AUDIOプレーヤ(これは、後述するデジタルデータ再生装置400を意味するものではない)により曲として認識され再生されるが、超流通ヘッダ及び超流通コンテンツは、そのような管理情報にて管理されていないため、CDプレーヤ、DVD-AUDIOプレーヤにより曲として認識され再生されることはない。これはCDプレーヤ、DVD-AUDIOプレーヤが、超流通ヘッダ及び超流通コンテンツを、販売目的コンテンツ同様そのまま再生しようとすると、CDプレーヤ、DVD-AUDIOプレーヤは超流

通ヘッダ及び超流通コンテンツを復号することができず、無意味で耳障りな音声が出力されてしまうので、そのように超流通ヘッダ及び超流通コンテンツが販売目的コンテンツと同様に再生されることを避けるためである。このようなCD、DVD-AUDIOにおける管理情報に代えて、超流通ヘッダ及び超流通コンテンツには、自身を販売目的コンテンツと区別するための固有の管理情報にて管理されており、専用装置が超流通ヘッダ及び超流通コンテンツを読み出す場合、この固有の管理情報にて、超流通ヘッダ及び超流通コンテンツについての記録開始位置ー記録終了位置は特定される。

【0036】続いて、これら販売目的コンテンツ3及び超流通コンテンツ10がどのようにして消費者に行き渡るか、超流通コンテンツ10の超流通がどのように行われるかを図6を参照しながら明らかにしてゆく。図6は、本実施形態における販売目的コンテンツ3と、超流通コンテンツ10とがどのように流通されるかを示す図である。図6において販売用記録媒体は、矢印y1に示すように音楽会社の直営工場に設置されたデジタルデータ記録装置100が販売目的コンテンツ3と、再生制御スクリプト4と、静止画データ5と、コンテナ6と、を記録媒体200に記録することにより、製造される。このようにして製造された販売用記録媒体200は、通常のCD同様、矢印y2に示すようにトラックの運送等の流通経路を経て、小売りの店頭で販売される。一般の消費者は、矢印y3に示すように販売されている販売用記録媒体200を購入することができる。

【0037】販売用記録媒体200を購入した消費者は、販売目的コンテンツ3を通常のCD、DVD-AUDIO同様のスタイルで鑑賞することができる。即ち、本図の矢印y4に示すように、歩行中に携帯型の再生装置に再生させることにより、販売目的コンテンツ3を鑑賞することができる。ここで消費者の家庭内には、通信回線に接続された専用装置として、デジタルデータ記録装置300やデジタルデータ再生装置400が設置されているものとする。このうちデジタルデータ記録装置300は、販売用記録媒体200に記録されている超流通コンテンツ10を有償で他の記録媒体に記録させるものであり、デジタルデータ再生装置400は、販売用記録媒体200に記録されている超流通コンテンツ10を有償で再生させるものである。また販売用記録媒体200に記録されている静止画データ5、再生制御スクリプト4は、図8に示す対話画面をこれらデジタルデータ記録装置300、デジタルデータ再生装置に表示させるものである。図8は、再生制御スクリプト4及び静止画データ5にて再生装置の表示画面に表示される対話画面の一例を示す図である。図8における対話画面は、ライブ演奏の様子等、超流通コンテンツ10を紹介する画像m1と、超流通コンテンツ10の再生を推薦する旨のメッセージm2と、その再生に対しての賛同又は拒否を指定できるボタンm3、m1

(図2) 00-196585 (P2000-196585A)

3と、再生価格の額m4と、当該楽譜の購入を推薦する旨を記述した文字列m5と、その購入に対しての賛同又は拒否を指定できるボタンm6、m16と、その購入価格m7とを含んでおり、超流通コンテンツ10の有償購入及び有償再生を推薦する内容になっていることがわかる。この対話画面にて、消費者がEnhanced-CDのコンテナ6内にどのような超流通コンテンツ10が収録されているかを知得し、もしそれらに興味があれば、消費者は、デジタルデータ記録装置300を用いてこの超流通コンテンツ10を買い取ることができ、またデジタルデータ再生装置を用いてこの超流通コンテンツ10を再生させることができる。超流通コンテンツ10を買い取った際、超流通コンテンツ10を再生させた際、デジタルデータ記録装置300、デジタルデータ再生装置400は、公衆回線を通じて必要な課金額を示す課金情報を送信する。送信された課金情報は、音楽センタの課金センタに設置してあるホストコンピュータ600に伝送される。

【0038】図7(a)～図7(d)は、デジタルデータ記録装置300を介して、販売用記録媒体200から買取用途の記録媒体へのコピーを行う様子を示す図である。ここで買取用途の記録媒体としては、DVD-RAMを用いるものとする。図7(a)においてデジタルデータ記録装置300に販売用記録媒体200、買取用途の記録媒体650がセットされると、図7(b)に示すように、デジタルデータ記録装置300の操作者は、販売用記録媒体200に記録されている著作物を買取用途の記録媒体650にコピーする。その後、買取用途の記録媒体650であるDVD-RAMを図7(c)に示すようにイジェクトすれば、超流通コンテンツ10の買い取りが完了する。このような買い取り後、DVD-RAMのカートリッジからDVD-RAMを取り出せば、DVD-RAMに記録されたコンテンツは、DVD-RAM対応型のDVD-Audioプレーヤを用いることにより再生される。ここで、DVD-RAM対応型のDVD-Audioプレーヤとは、DVD-Audioディスクのみならず、DVD-RAMの再生を行うことができるDVD-Audioプレーヤをいう。

【0039】尚、本実施形態では、デジタルデータ記録装置300は、超流通コンテンツをDVD-RAMに記録したが、メモ리카ードに記録してもよい。以上のような超流通において、超流通コンテンツ10に対する課金額は、販売目的コンテンツ3の小売り価格と比較して、割安に設定することができる。何故なら、販売目的コンテンツ3の小売り価格には、Enhanced-CD及びDVD-AUDIOの運送費等、Enhanced-CD及びDVD-AUDIOの流通に係る様々な流通コストが計上されているのに対して、超流通コンテンツ10の買い取りは、単に暗号化を解除するだけで良く、そのような流通コストが一切不要となるためである。

【0040】以上のように本実施形態によれば、インターネット等に代表される電子データ配信のためのインフ

ラストラクチャが整備されていない状況にあっても、関連する楽譜の売り込み等、電子音楽配信に近い形態で、対話的な音楽コンテンツの販売を行うことができる。

尚、本実施形態では音楽を記録する記録媒体としてEnhanced-CDと、DVD-AUDIOとを用いたが、ハイブリッドタイプのDVD-AUDIO(DVD-AUDIO、DVD-ROMの機能を兼備したディスク)を用いてもよい。更に本実施形態では、販売用途の記録媒体に超流通コンテンツ及び超流通ヘッダを含むコンテナを記録するものとして説明を行ったが、無償配布される記録媒体に超流通コンテンツ及び超流通ヘッダを含むコンテナを記録してもよい。

【0041】以上で、本発明の記録媒体に記録される第1実施形態、すなわち超流通形式のデータ構造の説明を終わる。

(第2実施形態) 第2実施形態は、超流通形式のデータを記録媒体に記録するデジタルデータ記録装置100に関する。図9に、第2実施形態に係わるデジタルデータ記録装置100の構成を示す。第2実施形態のデジタルデータ記録装置100は、汎用のパーソナルコンピュータに専用のアプリケーションプログラムをインストールすることにより実現され、入力部101、制御部102、エンコード部103、コンテンツ格納部104、取り出し部105、超流通コンテンツ暗号化部106、超流通ヘッダ暗号化部107、販売目的コンテンツ暗号化部108、記録部109、固有情報取り出し部110を備え、超流通コンテンツを販売用途の記録媒体200に記録する。以後、これらの構成要素についての説明を行う。

【0042】なお、本実施形態では、以後、記録対象を音楽コンテンツであるとするが、これに限られるものではなく、映像データや文字データ、あるいはこれらの組み合わせのデータでもよい。また販売用途の記録媒体200に記録されるべきデータとして、第1実施形態では、再生制御スクリプト4や静止画データ5を例示したが、これらが記録される手順については、本実施形態の主眼と異なるので説明を省略する。

【0043】入力部101は、マウス、キーボード等のポインティングデバイスと接続されており、操作者の指示を受け付ける。ここで、操作者の指示とは、音楽コンテンツのエンコードの指示、あるいは、エンコードしたデータの取り出し要求などが挙げられる。制御部102は、入力部101の要求を解釈し、音楽コンテンツをエンコードすることを後述するエンコード部103へ指示する。あるいは、後述するコンテンツ格納部104に記録されている音楽コンテンツを取り出すことを、やはり後述する取り出し部105へ指示する。

【0044】エンコード部103は、図示しないマスターテープ等に記録されている原音を例えばLPCM形式のデジタルデータに符号化し、AAC形式に圧縮して音楽コンテンツを生成する。その後第1実施形態に示したコンテ

(図3) 100-196585 (P2000-196585A)

ンツID11を生成する。尚、デジタルデータ記録装置100においてエンコード部103は必須ではない。何故なら、外部の業者に音楽コンテンツのエンコードを依頼し、エンコードされたデータをコンテンツ格納部104に記録する場合、エンコード部103は不必要となるからである。

【0045】コンテンツ格納部104は、大容量のハードディスク装置であって、エンコード部103のエンコードにより得られた音楽コンテンツ、及び、第1実施形態に示したコンテンツID11を格納する。取り出し部105は、制御部102からの指示に基づいて、エンコードにより得られた音楽コンテンツ並びに第1実施形態に示したコンテンツID11をコンテンツ格納部104から取り出す。

【0046】超流通コンテンツ暗号化部106は、第1実施形態で説明した復号鍵13を用いて超流通コンテンツ10を暗号化することにより、暗号化コンテンツ8を生成する。ここで、復号鍵13は、本デジタルデータ記録装置100の操作者が自由に設定することができる。超流通ヘッダ暗号化部107は、操作者により記述された超流通形式のデータの購入条件12と、コンテンツID11と、復号鍵13とを結合させて超流通ヘッダ9を得て、これを暗号化することにより、暗号化ヘッダ7を得る。さらに、生成した暗号化ヘッダ7を超流通コンテンツ暗号化部106が暗号化した暗号化コンテンツ8に付与してコンテナ6を得る。

【0047】固有情報取り出し部110は、販売用記録媒体200がDVD-AUDIOであり、販売目的コンテンツ3を記録媒体固有の識別情報に基づいて暗号化する場合、販売用途の記録媒体200の製造時にあらかじめ記録されている媒体固有の識別情報を取り出し、販売目的コンテンツ暗号化部108に出力する。尚、販売用記録媒体200がEnhanced-CDであり、販売目的コンテンツ3を暗号化する必要がない場合、媒体固有の識別情報を取り出しは行わない。

【0048】販売目的コンテンツ暗号化部108は、販売用記録媒体200がDVD-AUDIOである場合、販売目的コンテンツ3を、記録媒体固有の識別情報に基づいて暗号化する。尚、販売用記録媒体200がEnhanced-CDであり、販売目的コンテンツ3を暗号化する必要がない場合、販売目的コンテンツ暗号化部108は暗号化を行わない。尚、媒体固有の識別情報に基づいて暗号化する技術については、特開平5-257816号公報に開示されているので、ここでは詳しい説明は省略する。

【0049】記録部109は、超流通ヘッダ暗号化部107により生成されたコンテナ6と、第二の暗号化部108で暗号化された販売目的コンテンツとを記録する。以上のように構成されたデジタルデータ記録装置に関して、以後図10の処理内容を示すフローチャートを用いてその動作を説明する。なお、以下の動作に関しては、

すでにエンコード部103により、原音のエンコードが完了していて、コンテンツ格納部104に複数の音楽コンテンツが得られているものとする。

【0050】制御部102が起動されると、ステップS1において制御部102は、コンテンツ格納部104に格納している複数のコンテンツのうち、販売用途の記録媒体200に記録すべきものの選択を待つ。コンテンツが選択されれば、ステップS2において制御部102は操作者からの音楽コンテンツを販売用途の記録媒体200への記録指示を待つ。ここでの記録指示には、販売を目的として記録する旨の記録指示と、超流通を目的として記録する旨の記録指示とがある。記録指示があった場合、制御部102は、ステップS3においてそれが販売目的で記録する旨の記録指示か、それとも超流通形式での記録指示かを判定する。

【0051】操作者が販売用途のコンテンツの記録指示を行った場合、ステップS3において、販売用途のコンテンツの記録指示がなされたと判定される。この場合、制御部102は、ステップS3からステップS8に移行し、ステップS8において販売用途の記録媒体200のタイプがDVD-AUDIOであるか、Enhanced-CDであるかを判定する。Enhanced-CDなら、ステップS8からステップS6に移行して、取り出し部105に、選択された音楽コンテンツ及びコンテンツIDの取り出しを指示し、取り出された音楽コンテンツ及びコンテンツIDを販売用途の記録媒体200に記録させる。一方、DVD-AUDIOなら、ステップS8からステップS9へと移行する。ステップS9において制御部102は、取り出し部105に、適切な音楽コンテンツ及びコンテンツIDの取り出しを指示すると共に、取り出された音楽コンテンツを販売目的コンテンツ暗号化部108に引き渡す。販売目的コンテンツ暗号化部108は、販売用途の記録媒体200からの固有の識別情報の取り出しを、固有情報取り出し部110に指示し、これを受けた固有情報取り出し部110は、販売用途の記録媒体200から固有の識別情報を取り出す。その後、ステップS9からステップS10に移行して、販売目的コンテンツ暗号化部108は、固有情報取り出し部110により取り出された媒体固有の識別情報を暗号鍵として用いて暗号化を行なう。その後、ステップS10からステップS6に移行し、記録部109は、販売目的コンテンツ暗号化部108で暗号化された販売目的コンテンツ及びコンテンツIDを販売用途の記録媒体200に記録する。ステップS1からステップS6までの処理にて、販売目的コンテンツが販売用途の記録媒体200が記録されたので、続いて、超流通コンテンツの記録指示がなされた場合の動作について説明する。

【0052】記録指示が超流通形式であった場合は、制御部102は、取り出し部105に、選択された音楽コンテンツ及びコンテンツIDを取り出させて、コンテンツIDをヘッダ暗号化部107に出力させ、超流通コンテン

(図4) 100-196585 (P2000-196585A)

ツ暗号化部106に出力させる。超流通コンテンツ暗号化部106は、ステップS4において取り出されたコンテンツを暗号化することにより、暗号化コンテンツを生成する。更に制御部102は、ステップS5において超流通ヘッダ暗号化部107にコンテンツID11と、購入条件12と、復号鍵13とを結合させ、暗号化を行わせることにより、暗号化ヘッダ7を生成させて、暗号化ヘッダ7を暗号化コンテンツ8に付与させることによりコンテンツ6を生成する。その後、ステップS6に移行して、生成されたコンテンツ6を販売用途の記録媒体200に記録させる。記録媒体への記録が完了すると、ステップS7において、記録作業を終了するか否かを操作者に問い合わせ、もし終了するなら、本フローチャートにおける処理を終了する。続行するなら、ステップS7からステップS1に移行する。以上のように本実施形態によれば、販売用途の記録媒体200に記録すべき1つ以上のコンテンツのうち、その再生又は他の記録媒体への記録に対価の支払いが必要なものがあればこれを超流通コンテンツ10として選択して、これを暗号化するので、課金が行われていない間、超流通コンテンツ10についての再生又は他の記録媒体への記録を防止することができる。

【0053】超流通コンテンツ10を暗号化し、超流通コンテンツ10を再生又は買い取る場合に専用装置に課金を行わせる課金情報と、課金後に専用装置に超流通コンテンツ10の暗号化を解除させる復号鍵13を含む超流通ヘッダ9を超流通コンテンツ10に付与するので、超流通コンテンツ10の再生又は他の記録媒体への記録が行われる度に、音楽会社は収益を得ることができる。

【0054】以上で、第2実施形態の説明を終わる。(第3実施形態)次に、第3実施形態として、デジタルデータ記録装置300についての説明を行う。超流通コンテンツ10の買い取りという側面から、デジタルデータ記録装置300の内部構成を機能的に記述すれば、デジタルデータ記録装置300の内部構成は、図11に示すものとなる。図11は、第3実施形態のデジタルデータ記録装置300の内部構成を示す図である。デジタルデータ記録装置300は、本来電子音楽配信対応型のデジタルデータ記録装置であり、電子音楽配信におけるダウンロード機能、即ち、通信部313がコンテンツを有償でインターネットから受信して、買取用途の記録媒体650に記録する機能を有している。電子音楽配信対応型であるため、デジタルデータ記録装置300は、インターネットの通信を行うための通信部や、通信回線において電子商取引を行った場合に、通信回線上で金銭の決済を行うための課金部を有している。

【0055】図11において、第3実施形態のデジタルデータ記録装置300は、一般に汎用のパーソナルコンピュータに専用のアプリケーションプログラムをインス

トールすることにより実現され、入力部301、表示部302、制御部303、取り出し部304、超流通ヘッダ復号化部305、超流通コンテンツ復号化部306、固有情報取り出し部307、超流通コンテンツ再暗号化部308、記録部309、課金部310、課金情報格納部312、通信部313、及び記録回数管理部314を備える。

【0056】入力部301は、マウス、キーボード等のポインティングデバイスと接続されており、操作者からの曲の購入指示を受け付ける。『超流通』における曲の購入とは、『超流通形式のデータを別の記録媒体へ記録する』という行為が含まれる。ここで、デジタルデータ記録装置及びデジタルデータ再生装置にデジタル出力端子が備わっている場合、これらのデジタル出力端子にデジタル出力を行わせるという行為も『曲の購入』に含まれる。何故なら、このようなデジタル出力端子に、別の記録媒体のドライブ装置を接続すれば、このドライブ装置を用いて超流通コンテンツ10をこの記録媒体に記録させることができるからである。本実施形態において、デジタルデータ記録装置100は、デジタル出力端子を有しており、ケーブルを介してDVD-RAMのドライブ装置を接続している。

【0057】表示部302は、販売用途の記録媒体200に記録されている再生制御スクリプト4、静止画データ5に基づいて対話画面を表示することにより、超流通コンテンツ10の内容や、これを購入する際の対価の額等の情報を視覚的に提示する。制御部303は、入力部301を通じて入力された操作者の指示を解釈し、他の構成要素に指示を行う。あるいは、他の構成要素が出力した結果に応じて、次の処理の指示を行う。例えば、操作者から関連楽譜の購入指示があれば、後述する取り出し部304に、販売用途の記録媒体200に記録されている超流通コンテンツ10及び超流通ヘッダ9の取り出しを指示する。

【0058】取り出し部304は、第2実施形態に示した販売用途の記録媒体200に記録されているコンテンツ6を取り出す。超流通ヘッダ復号化部305は、取り出し部304がコンテンツ6を取り出すと、それに含まれるコンテンツ6内の暗号化ヘッダ7に対して復号鍵13を用いて復号化を行う。復号により超流通ヘッダ9が得られれば、これに含まれるコンテンツID11、購入条件12、復号鍵13を参照することにより、超流通コンテンツ10の購入条件を操作者に提示することができる。尚、超流通ヘッダを復号する際使用する復号鍵は、例えば、デジタルデータ記録装置300にインストールされているアプリケーションプログラムにあらかじめ格納されているもの、あるいは、通信回線を介して、課金センタから配布されるものを用いる。

【0059】超流通コンテンツ復号化部306は、超流通ヘッダ復号化部305が超流通ヘッダ9を復号化すれ

(図5)100-196585(P2000-196585A)

ば、これに含まれる復号鍵13を用いて、暗号化コンテンツ8を復号化する。固有情報取り出し部307は、買取用途の記録媒体650から、媒体固有の識別情報を取り出す。ここで買取用途の記録媒体650は、DVD-RAMであるので、BCA(Burst Cutting Area)に書かれた情報を媒体固有の識別情報として用いる。この媒体固有の識別情報は、ディスクごとにユニークであり、しかも通常ディスク製作時に記録される情報であって、書き換えることができない。したがって、万一悪意を持った操作者がディスクの内容を複製したとしても、復号鍵のもとになる識別情報が異なるために復号化することができず、データの著作権を確実に保護することが可能となる。

【0060】超流通コンテンツ再暗号化部308は、固有情報取り出し部307が取り出した買取用途の記録媒体650媒体固有の識別情報に基づき、超流通コンテンツ復号化部306が復号化した超流通コンテンツ10を暗号化する。記録部309は、超流通コンテンツ再暗号化部308により暗号化された超流通コンテンツ10を買取用途の記録媒体650に記録する。

【0061】課金部310は、記録部309の処理の終了通知があると、超流通ヘッダ復号化部305が超流通ヘッダ9を復号することにより得られた購入条件12から、課金情報を読み出して、その課金情報に基づいた課金額を算出し、課金情報に組み入れる。課金情報格納部312は、パーソナルコンピュータのハードディスクに相当し、課金部310が算出した課金額を含む課金情報を格納する。ここで、課金情報は、悪意を持った操作者が改竄することを防ぐ必要があるので、課金情報は、暗号化した状態でハードディスクに格納したり、ハードディスクにおけるセキュア領域(操作者の通常の操作では、アクセスできない領域)に格納することが望ましい。

【0062】通信部313は、通信回線に接続されたモデム装置と、その制御ソフトウェアとで構成され、課金情報格納部312に記録された課金情報と、操作者の操作者IDとを適当なタイミングにおいて、音楽センタの課金センタに設置してあるホストコンピュータ600に通信回線を介して送信する。ここで、適当なタイミングとは例えば、課金額がある一定値に達したときや、一定の期日に達したときなどが考えられる。勿論、操作者が買取用途の記録媒体650に記録するたびにホストコンピュータに接続するとしてもよい。

【0063】記録回数管理部314は、記録部309が買取用途の記録媒体650に、同一超流通コンテンツ10を記録した記録回数を記憶しており、記録部309が買取用途の記録媒体650に同一超流通コンテンツ10を記録する度に、この記録回数をインクリメントする。以上のように構成されたデジタルデータ記録装置の動作について、以後図12の処理内容を示すフローチャート

を用いて更に詳細に説明する。

【0064】制御部303は、販売用途の記録媒体200が装填されると、本フローチャートの処理を開始し、ステップS20において関連楽譜の紹介を希望する旨の操作が行われるのを待つ。そのような操作が行われれば、ステップS21において取り出し部304がその販売用途の記録媒体200の付加価値領域2から再生制御スクリプト4及び静止画データ5を読み出して、図8に示した対話画面を表示部302に表示させる。その後、ステップS22に移行して、操作者から超流通コンテンツ10の購入指示が行われるのを待つ。操作者がキャンセル操作を行った場合は、処理を終了するが、購入指示を行った場合、ステップS22からステップS23に移行して、取り出し部304に、販売用途の記録媒体200から、暗号化されたままの暗号化ヘッダ7を含むコンテンツ6を取り出させる。その後、ステップS24において、取り出されたコンテンツ6における暗号化ヘッダ7を復号化することにより、超流通ヘッダ9を得る。超流通ヘッダ9が得られると、ステップS25において同一超流通コンテンツ10がこれまで記録された回数を記録回数管理部314から読み出す。それと共に、ステップS26において復号により得られた超流通ヘッダ9からデジタル出力許可回数を読み出す。デジタル出力許可回数が読み出されると、ステップS27においてこれまでの記録回数がデジタル出力許可回数に等しいか否かを判定する。もし等しければ、これ以上の超流通コンテンツ10のデジタル出力は許可し得ないので、そのまま処理を終了する。一方、これまでの記録回数がデジタル出力許可回数を下回るのなら、制御部303は、ステップS28において超流通コンテンツ復号化部306に超流通ヘッダ9内の復号鍵13を用いて、コンテンツにおける暗号化コンテンツ8を復号化させる。

【0065】復号が行われると、制御部303は、ステップS29において固有情報取り出し部307に買取用途の記録媒体650から媒体固有の識別情報を取得させ、超流通コンテンツ再暗号化部308に、取得した識別情報を暗号鍵としてデータを暗号化させる。その後、ステップS30に移行して、記録部309により暗号化されたデータを買取用途の記録媒体650に記録させる。

【0066】記録部309による記録が完了すると、ステップS31において制御部303は、課金部310に購入条件12中の買い取り価格情報に基づいて、課金額を算出させ、課金情報格納部312に課金情報として格納させる。課金情報を格納させた後、ステップS32において課金情報を伝送するのに適当なタイミングが到来するのを待ち、そのようなタイミングが到来すれば、ステップS33において制御部303は通信部313に、課金情報格納部312に記録された課金情報と、操作者IDとを取り出させ、課金センタ内のホストコンピュータ

(図6) 100-196585 (P2000-196585A)

600に送信させて、処理を終了する。

【0067】以上のように本実施形態によれば、販売用途の記録媒体200を取得した消費者が、この超流通コンテンツ10の有償での購入に合意した場合のみ、販売用途の記録媒体200に記録されている超流通コンテンツ10を買取用途の記録媒体650に記録し、この記録行為に対する対価の額を示す課金情報のみを通信回線を介して課金センターに伝送させるので、超流通コンテンツ10を通信回線に伝送させる必要は無い。故に、通信回線の伝送速度が遅く、電子音楽配信のインフラストラクチャが整備されているとはいえない状態であっても、消費者が負担すべき通信料金は小額で済むので、超流通コンテンツ10の売買を安価に実現することができる。

【0068】以上で、第3実施形態の説明を終え、続いて第4実施形態の説明を行う。

(第4実施形態) 第4実施形態は、超流通コンテンツの有償での再生を行うデジタルデータ再生装置に関する。本デジタルデータ再生装置400は、販売用途の記録媒体200中の超流通形式のデータを他の記録媒体に記録せずに、そのまま復号化して再生する点が第3実施形態で説明したデジタルデータ記録装置300と大きく異なるが、デジタルデータ再生装置400は、第3実施形態におけるデジタルデータ記録装置300同様、電子音楽配信におけるダウンロード機能、即ち、コンテンツを有償でインターネットから受信する機能を有している。そのため、デジタルデータ再生装置は、デジタルデータ記録装置300と共通の構成要素を多く含んでいる。図13は、第4実施形態に係るデジタルデータ再生装置の構成を示す図である。図13におけるデジタルデータ再生装置の構成要素のうち、デジタルデータ記録装置300と共通の構成要素については、デジタルデータ記録装置300と同一の参照符号を付して説明を省略する。一方、デジタルデータ再生装置の構成要素のうち400番台の参照符号を付したもの(再生部401、再生回数管理部402)は、デジタルデータ記録装置300が具備していない、デジタルデータ再生装置400特有の構成要素であり、以降これらの構成要素について説明を行う。

【0069】図13における再生部401は、超流通コンテンツ復号化部306により復号化された超流通コンテンツ10を再生する。また、超流通コンテンツ10の再生を開始すると、その旨を課金部310に伝える。再生部401が再生開始を課金部310に伝達することにより、第4実施形態では、超流通コンテンツ10の再生が行われた際、適切な課金が行われる。

【0070】再生回数管理部402は、再生部401が同一の超流通コンテンツ10を再生した再生回数を記憶しており、再生部401が同一の超流通コンテンツ10を再生する度に、この再生回数をインクリメントする。以上のように構成されたデジタルデータ再生装置の動作

について、以後図1.4の処理内容を示すフローチャートを用いて更に詳細に説明する。

【0071】本フローチャートにおいてステップS20からステップS24まで、ステップS28、ステップS31からステップS33までのステップは、図12の処理内容を示すフローチャートと同一処理である。一方、ステップS41からステップS46までは、第4実施形態特有の処理なのでこれらのステップのみについて説明を行う。ステップS24において、取り出されたコンテンツナ6における暗号化ヘッダ7が復号化され、超流通ヘッダ9を得ると、ステップS41においてデジタルデータ再生装置の制御部303は、同一超流通コンテンツ10がこれまで再生された回数を再生回数管理部402から読み出す。それと共に、超流通ヘッダ9から再生許可回数を読み出す。再生許可回数が読み出されると、ステップS42において制御部303は、これまでの再生回数が再生許可回数を下回るか否かを判定し、もし等しければ、これ以上の超流通コンテンツ10の再生は許可し得ないので、そのまま処理を終了する。

【0072】これまでの再生回数が再生許可回数を下回るなら、ステップS43において現在日時を読み出し、ステップS44において制御部303は、再生許可時間及び再生許可期日を超流通ヘッダ9から読み出す。これらが読み出されると、ステップS45において現在日時が既に再生許可時間及び再生許可期日を経過しているかを判定する。経過していれば処理を終了するが、経過していなければ、ステップS45からステップS28に移行して、超流通コンテンツ復号化部306に、超流通ヘッダ9内の復号鍵13を用いて、コンテンツにおける暗号化コンテンツ8を復号化させる。その後、ステップS46において、超流通コンテンツ10を再生するよう再生部401を制御する。

【0073】以上のように本実施形態によれば、超流通コンテンツ10の再生開始時に、再生が開始した旨を課金部310に伝達するので、超流通コンテンツ10が再生される度に、音楽会社は収益を得ることができる。尚、第3実施形態における超流通コンテンツ10の買い取り機能と、超流通コンテンツ10の再生機能とを一体化させたデジタルデータ記録装置を構成しても良い。

【0074】以上で、第4実施形態の説明を終る。次に第5実施形態の説明を行う。

(第5実施形態) 第1実施形態～第4実施形態では、音楽コンテンツが記録媒体を用いて配布されることを想定していたが、第5実施形態では、記録媒体のみならず、インターネットや衛星放送やケーブルTV等の放送波にて音楽コンテンツが配布されることを想定している。図15は、第5実施形態における音楽コンテンツの配布形態を示す図である。本図において、コンテンツパッケージング装置700が作成した音楽コンテンツは、DVD-Audio 701、CD 702、インターネット 703、ケーブルT

(註7) 100-196585 (P2000-196585A)

V704、通信衛星705を介して配布されていることを示す図である。一方本図において、コンテンツ再生装置801～コンテンツ再生装置809は何れも、音楽コンテンツを再生する再生装置であり、音楽コンテンツ再生専用的高级機の再生装置801、音楽コンテンツ再生専用であるが低級機の再生装置802、803、音楽コンテンツ再生専用の携帯型の再生装置804、805、汎用のパソコンに専用のハードウェアを装着させた再生装置806、807、衛星放送やCATVの受信用のセットトップボックス型の再生装置808、809等がある。

【0075】音楽コンテンツの配布先となる再生装置には、上述したように様々なタイプのものがある。音楽コンテンツ再生専用の民生機器タイプの再生装置801、802等は、暗号化の解除を行うために専用ハードウェアを具備している。これに対して、汎用パソコン型の再生装置806、807等は、そのような専用ハードウェアを具備しておらず、汎用ハードウェア上で復号ソフトウェアを動作させることにより、暗号化の解除を行う。これらのことから、汎用パソコンなどは、著作権保護機構が未整備であり、民生機器タイプの再生装置は、著作権保護機構が整備済みであると言える。また、民生機器はコンテンツを再生する際の品質が高く、汎用パーソナルコンピュータはコンテンツを再生する際の品質が低い。故に、コンテンツの再生品質が高い再生装置は著作権保護機構が整備されており、コンテンツの再生品質が低い再生装置は著作権保護機構が未整備であることがわかる。

【0076】コンテンツパッケージング装置700及び再生装置801～809の内部構成を機能的に記述すると、図16のようになる。図16は、第5実施形態におけるコンテンツパッケージング装置700及びコンテンツ再生装置801～809の内部構成を示す図である。本図において、コンテンツパッケージング装置700は、コンテンツ符号化部706、コンテンツ品質 暗号対応表格納部707、コンテンツ暗号化部708、コンテンツ梱包部709を含む。

【0077】コンテンツ符号化部706は、配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る。この符号化により、販売用コンテンツ710と、販売用コンテンツよりも品質の劣る低い品質で再生される試供用コンテンツ711とが得られるものとする。コンテンツ品質 暗号対応表格納部707は、コンテンツを符号化する際の量子化ビット数及びサンプリング周波数と、この量子化ビット数及びサンプリング周波数のコンテンツに付与されるべきランクと対応づけた第1対応表と、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした第2対応表とを格納する。

【0078】第1対応表の一例を図17(a)に示す。図17(a)に示すように、第1対応表におけるランク

1には、24bitといった量子化ビット数と、96KHzといったサンプリング周波数とが対応づけられており、ランク2には、16bitといった量子化ビット数と、44.1KHzといったサンプリング周波数、ランク3には、16bitといった量子化ビット数と、22.05KHzといったサンプリング周波数とが対応づけられていることがわかる。このように量子化ビット数及びサンプリング周波数が高ければ高い程、対応づけられているランク値は高いことがわかる（ここで、ランク値は、数値が少ない程、ランクが高いことを意味している）。

【0079】第2対応表の一例を図17(b)に示す。図17(b)に示すように、第2対応表におけるランク1には、1024bitといった暗号鍵と、RSAといった暗号化アルゴリズムとが対応づけられており、ランク2には、512bitといった暗号鍵と、RSAといった暗号化アルゴリズム、ランク3には、56bitといった暗号鍵と、DESといった暗号化アルゴリズムとが対応づけられていることがわかる。これらの暗号化アルゴリズムのうち、RSAはDESより安全性が高く、暗号鍵のビット長が長い程、安全性は高いので、このようにランク値が高ければ高い程、対応づけられている暗号鍵及び暗号化アルゴリズムの安全性は高いことがわかる。

【0080】コンテンツ暗号化部708は、再生品質の高低に応じて、各コンテンツをランク付けし、ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する。例えば、パッケージの符号化により得られた販売用コンテンツ710が配布対象であり、24bitの量子化周波数と、96KHzのサンプリング周波数を有している場合、コンテンツ暗号化部708は、図17(a)に示す第1対応表に基づいて、販売用コンテンツ710に“1”のランク値を付与する。ランク値を付与した後、コンテンツ暗号化部708は、第2対応表における暗号鍵欄を参照して、ランク1に対応する暗号鍵として、1024bitの暗号鍵（セッションキー）を生成する。その後、コンテンツ暗号化部708は、第2対応表における暗号化アルゴリズム欄を参照して、当該1024bit長の暗号鍵を公開鍵暗号アルゴリズム（RSA）にて暗号化して、上記スクランブル処理が施された販売用コンテンツに添付する。

【0081】一方、試供用コンテンツ711が配布対象であり、16bitの量子化周波数と、44.1KHzのサンプリング周波数を有している場合、コンテンツ暗号化部708は、図17(a)に示す第1対応表に基づいて、販売用コンテンツ710に“2”のランク値を付与する。ランク値を付与した後、コンテンツ暗号化部708は、第2対応表における暗号鍵欄を参照して、ランク2に対応する暗号鍵として、512bitの暗号鍵（セッションキー）を生成する。その後、コンテンツ暗号化部708は、第2対応表における暗号化アルゴリズム欄を参照して、当該512bit長の暗号鍵を公開鍵暗号アルゴリズム（RSA）にて

(註 8) 100-196585 (P2000-196585A)

暗号化して、上記スクランブル処理が施された試供用コンテンツに添付する。

【0082】コンテンツ梱包部709は、コンテンツ暗号化部708により暗号化された販売用コンテンツ710及び試供用コンテンツ711を梱包し、配布形態に応じたパッケージを得る。音楽コンテンツの配布形態がインターネット、衛星放送、CATV等である場合、コンテンツ梱包部709は、このパッケージをTCPパケット、トランスポートパケットに変換して出力する。また、音楽コンテンツの配布形態がCD-ROM、DVD-ROMなどの記録媒体である場合、コンテンツ梱包部709は、パッケージをUDF形式(ユニバーサルディスクフォーマット)等の形式のファイルに変換して、CD-ROM、DVD-ROMに記録する。このようにパッケージが記録されれば、図18に示すように、複数のコンテンツを含むパッケージが様々な再生装置に配布されることになる。図18は、第7実施形態におけるコンテンツ梱包部709が梱包を行うことにより得られたパッケージを示す図である。

【0083】続いてコンテンツ再生装置801~809について説明する。図15に示したように、コンテンツ再生装置801~809は、それぞれ独自の形態を有しているが、図16に示すハードウェア性能 復号対応表格納部810、ハードウェア性能評価部811、コンテンツ開梱部812、コンテンツ復号化部813、コンテンツ格納部814、コンテンツ再生部815を含む点で共通している。

【0084】ハードウェア性能 復号対応表格納部810は、複数のランク値と、復号鍵及び復号アルゴリズムとを対応づけた対応表格納している。ここでコンテンツ品質 暗号対応表格納部707が格納している第1対応表、第2対応表におけるランク値は、コンテンツにおける再生品質の高低に応じた値を有していたが、ハードウェア性能 復号対応表格納部810に格納されている対応表におけるランク値は、再生装置801~808のそれぞれが有するハードウェア性能を評価するために用いられることに注意されたい。再生装置801~808のそれぞれが有するハードウェア性能とは、再生装置のハードウェアが、暗号化を復号するために専用ハードウェアを具備しているか否を示し、また著作権保護機構が整備されている場合、その暗号化の解除能力の高さを定量化した値であり、ハードウェア性能のランク値が高い程、その著作権保護機構が整備されていることを示し、ハードウェア性能のランク値が低い程、その著作権保護機構が未整備であることを示す。尚、本実施形態において、ハードウェア性能の評価のためのランク値はランク値A,B,Cという単位を用いて表現し、A→B→Cの順で、ハードウェア性能は高いものとする。図17(c)は、ハードウェア性能 復号対応表格納部810が格納しているハードウェア性能 復号対応表を示す図である。図17(c)の対応表におけるランクAは、著作権保護機構

が整備されていることを示しているが、このランクAには、1024bitといった復号鍵と、RSAといった復号化アルゴリズムとが対応づけられている。一方、ランクB,Cは、ランクAの再生装置と比較して、著作権保護機構が整備されていない再生装置に付与されるべきランク値である。ランク値Bには、56bitといった復号鍵と、RSAといった復号化アルゴリズム、ランクCには、56bitといった復号鍵と、DESといった復号化アルゴリズムとが対応づけられていることがわかる。

【0085】ハードウェア性能評価部811は、コンテンツの暗号化を復号するための専用ハードウェアの具備の有無を検出し、ハードウェアにおいて復号処理に用いることができるメモリ規模を算出することにより、再生装置のハードウェアの性能を評価して、当該ハードウェアの性能を示すランク値を算出する。コンテンツ開梱部812は、コンテンツパッケージング装置700によりパッケージが配布されれば、このパッケージを取得して、このパッケージから販売用コンテンツ、及び試供用コンテンツを抽出する。

【0086】コンテンツ復号化部813は、ハードウェア性能 復号対応表格納部810における複数の復号鍵及び復号アルゴリズムのうち、ハードウェア性能評価部811により評価されたランク値に応じたものを選択する。それと共に、コンテンツ開梱部812により抽出されたコンテンツのうち、選択された復号鍵及び復号アルゴリズムにて暗号化が解除されるべきコンテンツのみを分離して、分離されたコンテンツの暗号化を解除する。

【0087】ここで上述した民生機器の高級機器であるコンテンツ再生装置801が対象である場合、コンテンツ復号化部813によるコンテンツの復号がどのように行われるかについて説明する。このコンテンツ再生装置801は、暗号化を復号するための専用のハードウェアを有しているので、ハードウェア性能評価部811によりハードウェア性能がランクAと評価されることになる。またハードウェア性能 復号対応表格納部810においてランクAには、1024bitの復号鍵と、RSAの復号アルゴリズムとが対応づけられているので、コンテンツ復号化部813は1024bitの復号鍵と、RSAの復号アルゴリズムとを選択する。一方、販売用コンテンツ710は1024bitの暗号化鍵と、RSAの暗号化アルゴリズムを用いて暗号化されているので、コンテンツ復号化部813は、コンテンツ開梱部812がパッケージから抽出したコンテンツのうち、販売用コンテンツ710のみを分離する。そして、公開鍵暗号を解除するために予め配布されている復号鍵を用いて、復号化処理を行う。

【0088】続いて、汎用ハードウェア上で復号ソフトウェアを動作させることにより、暗号化の解除を行う汎用パーソナルコンピュータ型のコンテンツ再生装置806が対象である場合、コンテンツ復号化部813によるコンテンツの復号がどのように行われるかについて説

(9) 100-196585 (P 2000-196585A)

明する。このコンテンツ再生装置806は、汎用のハードウェアしか有していないので、ハードウェア性能評価部811によりハードウェア性能がランクCと評価されることになる。一方、ハードウェア性能 復号対応表格納部810においてランクCには、56bitの復号鍵と、DESの復号アルゴリズムとが対応づけられているので、コンテンツ復号化部813は、56bitの復号鍵と、DESの復号アルゴリズムとを選択する。一方、試供用コンテンツ711は56bitの暗号化鍵と、DESの暗号化アルゴリズムを用いて暗号化されているので、コンテンツ復号化部813は、コンテンツ開梱部812がパッケージから抽出したコンテンツのうち、試供用コンテンツ711のみを分離する。一方、DESは、共通鍵暗号なので、暗号化時に用いた暗号鍵により、コンテンツを復号することができる。よって、コンテンツ復号化部813は、当該パッケージから暗号鍵を取り出し、これを復号鍵として用いて、復号化処理を行う。

【0089】コンテンツ格納部814は、コンテンツ復号化部813により復号されたコンテンツを格納する。コンテンツ再生部815は、いったんコンテンツ格納手段723に格納された復号済みのコンテンツを再生する。以上のように本実施形態によれば、販売用コンテンツ710と、この販売用コンテンツ710より低い品質にて再生される試供用コンテンツ711とをそれぞれ異なるレベルの暗号化処理を施し、コンテンツ梱包手段713によって、パッケージとしてパッケージングするようにしたので、再生側では、ハードウェアの再生性能に応じたコンテンツが選択されて再生されるようになり、音楽コンテンツの配布先の再生装置に、汎用タイプ、高級タイプ等の差違がある場合、これに応じたコンテンツが再生されることになる。そのため、コンテンツを提供する側は、コンテンツの再生環境を考慮することなく、品質の異なるコンテンツを同時に提供することができ、また、コンテンツに対する著作権を安全に保護することができるようになる。

【0090】以上で第5実施形態の説明を終わる。次に第6実施形態の説明を行う。

(第6実施形態) 第6実施形態は、コンテンツ符号化部706が、配布対象の先頭部分を符号化することにより試供用コンテンツ711を得ると共に、配布対象の残りの部分を符号化することにより販売用コンテンツ710を得て、これをパッケージに梱包するというコンテンツパッケージング装置700の改良に関する。図19は、第6実施形態における、コンテンツパッケージング装置700と、コンテンツ再生装置801～809を示す図である。

【0091】本実施形態においてコンテンツ暗号化部708は、試供用コンテンツに所定のランクを付与し、差分コンテンツに、より高いランクを付与する。ランクが付与されたコンテンツを、対応表に示されているランク

に応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化して、コンテンツ梱包部709は、前記暗号化された複数のコンテンツを梱包して、パッケージを生成する。図20は、第7実施形態におけるコンテンツ梱包部709が梱包を行うことにより得られたパッケージを示す図である。

【0092】以上のように本実施形態によれば、コンテンツパッケージング時のパッケージの大きさを縮小することができ、その結果、伝送容量の低減、及びパッケージを記録する、例えば、ハードディスクやCD-ROMなどの記録媒体の容量節約を行うことができる等の利点がある。上記実施形態に基づいて説明してきたが、現状において最善の効果が期待できるシステム例として提示したに過ぎない。本発明はその要旨を逸脱しない範囲で変更実施することができる。代表的な変更実施の形態として、以下(a)～(f)に示すものがある。

【0093】(a) 第1実施形態～第4実施形態では、買取用途の記録媒体650を、DVD-RAMなどの光ディスクとして説明を行なったが、光ディスク以外のハードディスク、半導体メモリなどに置き換えてもよい。

(b) 第3～第4実施形態において課金情報を記録するときには、課金情報格納部312をパソコンのハードディスクとして説明を行なったが、ハードディスクに限られるものではなく、ICカードなどの記録媒体に置きかえることが可能である。

【0094】(c) 第1～第4実施形態においてデジタルデータ記録装置500については、パソコンで構成され家庭内で用いられることを想定して説明を行なったが、既存のレコード店などの店舗に設置してもよいことはいふまでもない。

(d) 第1～第4実施形態において、情報提供者が提供する情報を音楽コンテンツとして説明したが、これに限るものでなく、音楽コンテンツ、映像コンテンツ、文字情報、あるいは、映像コンテンツと音楽コンテンツと文字情報の組み合わせたものなどでもよいことはもちろんである。

【0095】(e) 第5実施形態において、販売用コンテンツ710と、試供用コンテンツ711とが配布されるものとしたが、これに限られるものではなく、さらに段階的な品質を有するコンテンツを用いて3つ以上のコンテンツを配信する場合においても適用することができる。

(f) 第1～第6実施形態において本実施形態でフローチャートを参照して説明した手順(図10、図12、図14)等を機械語プログラムにより実現し、これを記録媒体に記録して流通 販売の対象にしても良い。このような記録媒体には、ICカードや光ディスク、フロッピーディスク等があるが、これらに記録された機械語プログラムは汎用コンピュータにインストールされることにより利用に供される。この汎用コンピュータは、インスト

(20) 00-196585 (P2000-196585A)

ールした機械語プログラムを逐次実行して、本実施形態に示したデジタルデータ記録装置、デジタルデータ再生装置の機能を実現するのである。

【0096】

【発明の効果】以上説明したように本発明に係る記録媒体は、第1コンテンツと、第1コンテンツとは異なるコンテンツであって、第1暗号方式に基づいて暗号化されている第2コンテンツと、第2コンテンツに対応づけられていて、第2コンテンツにおける暗号化を解除させるために用いられる第1鍵情報を含んでおり、所定の装置に予め配布されている第2鍵情報を用いた場合のみ、その暗号化の解除が行われる暗号方式である第2暗号方式にて暗号化されているヘッダとが記録されているので、第1コンテンツが有名アーティストの新譜であり、第2コンテンツが関連する楽譜であれば、この第1コンテンツを購入した消費者は、第1暗号方式、第2暗号方式の暗号化を解除することにより、この関連する楽譜の音楽コンテンツを入手することができる。この暗号化の解除は、その暗号化を解除させるための第2鍵情報が予め配布されている所定の装置に、本記録媒体を装填すればよいので、消費者は、そのような所定の装置を自宅に有していれば、長時間をかけてコンテンツをダウンロードしなくてもよい。また、第2コンテンツを購入するためにわざわざコンテンツの小売り店に出向かなくてもよい。このように、消費者は、有名アーティストの新譜に関連する楽譜を簡易に入手することができる。

【0097】また運送費等、記録媒体の流通に係る様々な流通コストは、この記録媒体一枚に対して計上されるので、音楽会社は第2コンテンツに対する課金額は割安に設定することができ、消費者は安価に第2コンテンツを入手することができる。ここで、有償で再生又は買い取りを行うべき第2コンテンツを不正な再生や記録から防御するためには、公開鍵利用のアルゴリズム等、処理負荷が重く、安全性が高いアルゴリズムで第2コンテンツを暗号化せねばならず、第2コンテンツが数メガバイトというデータサイズを有している場合は、その暗号化の解除に要する時間が長時間になることが懸念されるが、本発明に係る記録媒体は、第2コンテンツ自体が第1暗号方式にて暗号化され、ヘッダが第2暗号方式にて暗号化されるので、第2暗号方式が公開鍵利用のアルゴリズムである場合、公開鍵利用のアルゴリズムにて暗号化する箇所を、ヘッダのみに絞ることができる。

【0098】このように安全性が高いアルゴリズムにて暗号化する箇所をヘッダのみに絞り、その中に第1コンテンツの暗号化を解除するための第1鍵情報を格納しておくので、第2コンテンツ自体を公開鍵利用のアルゴリズムで暗号化する場合と比較して、第2コンテンツにおける暗号化を解除するまでの時間を短くすることができる。これにより超流通コンテンツの買取や再生を指示してから、買取や再生が可能となるまでの時間は短くて済

むので、超流通コンテンツの購入を希望した者を悪戯に苛立たせることはなく、購入をキャンセルする確率は低くなる。この解除に要する時間は、電子音楽配信における音楽コンテンツのダウンロードに要する時間より極めて短くなると考えられるので、操作者は、買取又は再生を希望した超流通コンテンツをすぐさま鑑賞することができる。

【0099】ここで前記所定装置は、課金を行う機能を有しており、前記ヘッダは更に、第2コンテンツの再生又は他の記録媒体への記録を許諾するか否かと、再生又は他の記録媒体への記録を許諾する場合の上限回数とを示す利用制限情報と、第2コンテンツの再生又は他の記録媒体に記録が許諾されている場合に、前記所定装置に課金させるべき再生に要する料金又は他の記録媒体への記録に要する料金を示す課金情報とを含んでいても良い。

【0100】この記録媒体によれば、例えば第2コンテンツが他の記録媒体に記録されることや第2コンテンツが再生されることを無限に許可するのではなく、上限を設定できるので、第2コンテンツの複製が氾濫することや、第2コンテンツの再生が頻繁に行われて第2コンテンツが陳腐化するのを防止することができる。ここで前記所定装置は、課金を行う機能を有しており、前記ヘッダは更に、第2コンテンツの再生又は他の記録媒体への記録を許諾するか否かと、再生又は他の記録媒体に記録を許諾する場合の許可期間を示す許可期間情報と、第2コンテンツの再生又は他の記録媒体に記録が許諾されている場合に、前記所定装置に課金させるべき再生に要する料金又は他の記録媒体への記録に要する料金を示す課金情報とを含んでいてもよい。

【0101】この記録媒体によれば、その許可期間情報に示されている期間しか第2コンテンツの複製又は再生を許諾は行なえないので、季節限定、期間限定等のプレミア的な付加価値を第2コンテンツに与えることができる。ここで記録媒体に記録すべきコンテンツを少なくとも1つ以上格納する格納手段と、その再生又は他の記録媒体への記録に課金を行うべきものが前記1つ以上のコンテンツに存在する場合、そのコンテンツを超流通コンテンツとして選択する選択手段と、課金が行われていない間、選択された超流通コンテンツについての再生又は他の記録媒体への記録を防止するよう、第1暗号方式に基づいて超流通コンテンツを暗号化する第1暗号化手段と、超流通コンテンツの暗号化を解除させる鍵情報を含む超流通ヘッダを生成する生成手段と、生成された超流通ヘッダを、前記第1暗号方式より安全性が高い第2暗号方式に基づいて暗号化して、超流通コンテンツに付与する第2暗号化手段と、超流通ヘッダが付与されると、1つ以上のコンテンツをデジタルデータとして記録媒体に記録する記録手段とを備えることを特徴とするデジタルデータ記録装置を用いてもよい。

(21) 00-196585 (P2000-196585A)

【0102】このデジタルデータ記録装置によれば、販売用途の記録媒体に記録すべき1つ以上のコンテンツのうち、その再生又は他の記録媒体への記録に対価の支払いが必要なものがあればこれを超流通コンテンツとして選択して、これを暗号化するので、課金が行われていない間、超流通コンテンツについての再生又は他の記録媒体への記録を防止することができる。

【0103】超流通コンテンツを暗号化し、超流通コンテンツに対する対価を示す課金情報と、対価が支払われた場合に、超流通コンテンツの再生装置に超流通コンテンツの暗号化を解除させるコンテンツキーとを含む超流通ヘッダを超流通コンテンツに付与するので、超流通コンテンツの再生又は他の記録媒体への記録が行われる度に、音楽会社は収益を得ることができる。

【0104】ここで第1記録媒体及び第2記録媒体の少なくとも一方を装填する装填手段と、装填手段に装填された記録媒体が第1記録媒体であれば、超流通コンテンツを第1記録媒体から読み出す読出手段と、超流通コンテンツの第2記録媒体への記録に対する対価を操作者に提示する提示手段と、操作者からの操作を受け付ける受付手段と、受付手段が受け付けた操作が、対価の支払いに同意する旨の操作である場合、第1記録媒体から読み出された超流通コンテンツの暗号化を解除する解除手段と、対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金手段と、装填手段に超流通コンテンツの記録先となる第2記録媒体が装填されれば、暗号化が解除された超流通コンテンツをデジタルデータとして記録先の第2記録媒体に記録する記録手段とを備えるデジタルデータ記録装置を用いてもよい。

【0105】このデジタルデータ記録装置によれば、記録媒体を取得した消費者が、この超流通コンテンツの対価の支払いに合意した場合のみ、記録媒体に記録されている超流通コンテンツを買取用途の記録媒体に記録し、この記録行為に対しての課金を行うので、超流通コンテンツを回線に伝送させる必要は無い。故に、回線の伝送速度が遅く、電子音楽配信のインフラストラクチャが充分整備されているとはいえない状態であっても、消費者が負担すべき通信料金は小額で済むので、超流通コンテンツの売買を安価に実現することができる。

【0106】ここで記録媒体を装填する装填手段と、装填手段に装填された記録媒体に超流通コンテンツが記録されていればこれを読み出す読出手段と、超流通コンテンツの再生に対する対価を操作者に提示する提示手段と、操作者からの操作を受け付ける受付手段と、受付手段が受け付けた操作が、対価の支払いに同意する旨の操作である場合、超流通コンテンツの暗号化を解除する解除手段と、対価の支払いに同意する旨の指示を操作者から受け付けた場合、操作者に対して課金を行う課金手段と、暗号化が解除された超流通コンテンツを再生する再

生手段とを備えるデジタルデータ再生装置を用いてもよい。

【0107】このデジタルデータ再生装置によれば、超流通コンテンツの再生開始時に、課金を行うので、超流通コンテンツが再生される度に、音楽会社は収益を得ることができる。ここで配布対象を異なる方式にて符号化することにより、再生時の品質が異なるコンテンツを複数得る符号化手段と、再生品質の高低に応じて、各コンテンツをランク付けするランク付け手段と、複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にした対応表を格納する対応表格納手段と、ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化手段と、前記暗号化された複数のコンテンツを含むパッケージを生成する梱包手段とを備えるコンテンツパッケージング装置を用いてもよい。

【0108】このコンテンツパッケージング装置によれば、販売用コンテンツと、この販売用コンテンツより低い品質にて再生される試供用コンテンツとをそれぞれ異なるレベルの暗号化処理を施し、コンテンツ梱包手段によって、パッケージとしてパッケージングするようにしたので、再生側では、ハードウェアの再生性能に応じたコンテンツが選択されて再生されるようになり、音楽コンテンツの配布先の再生装置に、汎用タイプ、高級タイプ等、様々なタイプが存在する場合、これに応じたコンテンツが再生されることになる。そのため、コンテンツを提供する側は、コンテンツの再生環境を考慮することなく、品質の異なるコンテンツを同時に提供することができ、また、コンテンツに対する著作権を安全に保護することができるようになる。

【0109】ここで、配布対象の一部を符号化することにより試供用コンテンツを得ると共に、配布対象の残りの部分を符号化することにより差分コンテンツを得る符号化手段と、試供用コンテンツに所定のランクを付与し、差分コンテンツに、より高いランクを付与するランク付け手段と、複数のランクと、各ランクのコンテンツを暗号化するために用いるべき暗号鍵及び暗号アルゴリズムとを組にしており、一方の組には、所定のランクが対応づけられ、他方の組には、当該所定のランクより高いランクに対応づけられている対応表格納している対応表格納手段と、ランクが付与されたコンテンツを、対応表に示されているランクに応じた暗号鍵及び暗号化アルゴリズムを用いて暗号化する暗号化手段と、前記暗号化された複数のコンテンツを含むパッケージを生成する梱包手段とを備えるコンテンツパッケージング装置を用いてもよい。

【0110】このコンテンツパッケージング装置によれば、コンテンツをパッケージングする際のパッケージの大きさを縮小することができ、その結果、伝送容量の低

(22) 00-196585 (P2000-196585A)

減、及びパッケージを記録する、例えば、ハードディスクやCD-ROMなどの記録媒体の容量節約を行うことができる等の利点がある。

【図面の簡単な説明】

【図1】(a) Enhanced-CDの外観を示す図である。

(b) Enhanced-CDの物理構造を示す図である。

【図2】(a) DVD-AUDIOの外観を示す図である。

(b) DVD-AUDIOの機能的なフォーマットを示す図である。

【図3】販売用記録媒体を収納した専用のプラスチックケースを示す図である。

【図4】コンテナ6のデータ構造を示す図である。

【図5】購入条件12の一例を示す図である。

【図6】本実施形態における販売目的コンテンツ3と、超流通コンテンツ10とがどのように流通されるかを示す図である。

【図7】(a)～(d) 販売用記録媒体200から買取用途の記録媒体650へと超流通コンテンツが買い取られる手順を示す図である。

【図8】再生制御スクリプト4及び静止画データ5にて再生装置の表示画面に表示される対話画面の一例を示す図である。

【図9】第2実施形態に係わるデジタルデータ記録装置100の構成を示す図である。

【図10】第2実施形態のデジタルデータ記録装置100の処理内容を示すフローチャートである。

【図11】第3実施形態のデジタルデータ記録装置300の内部構成を示す図である。

【図12】第3実施形態のデジタルデータ記録装置300の処理内容を示すフローチャートである。

【図13】第4実施形態のデジタルデータ再生装置400の内部構成を示す図である。

【図14】第4実施形態のデジタルデータ再生装置400の処理内容を示すフローチャートである。

【図15】第5実施形態における音楽コンテンツの配布形態を示す図である。

【図16】第5実施形態におけるコンテンツパッケージング装置700及びコンテンツ再生装置801～809の内部構成を示す図である。

【図17】(a) 第1対応表の一例を示す図である。

(b) 第2対応表の一例を示す図である。

(c) ハードウェア性能 復号対応表の一例を示す図である。

【図18】第5実施形態におけるコンテンツ梱包部709が梱包を行うことにより得られたパッケージを示す図である。

【図19】第6実施形態におけるコンテンツパッケージング装置700及びコンテンツ再生装置801～809の内部構成を示す図である。

【図20】第6実施形態におけるコンテンツ梱包部70

9が梱包を行うことにより得られたパッケージを示す図である。

【符号の説明】

- 1 コンテンツ領域
- 2 付加価値領域
- 3 販売目的コンテンツ
- 4 再生制御スクリプト
- 5 静止画データ
- 6 コンテナ
- 7 暗号化ヘッダ
- 8 暗号化コンテンツ
- 9 超流通ヘッダ
- 10 超流通コンテンツ
- 11 コンテンツID
- 12 購入条件
- 13 復号鍵
- 100 デジタルデータ記録装置
- 101 入力部
- 102 制御部
- 103 エンコード部
- 104 コンテンツ格納部
- 105 取り出し部
- 106 超流通コンテンツ暗号化部
- 107 超流通ヘッダ暗号化部
- 108 販売目的コンテンツ暗号化部
- 109 記録部
- 110 固有情報取り出し部
- 200 販売用途の記録媒体
- 300 デジタルデータ記録装置
- 301 入力部
- 302 表示部
- 303 制御部
- 304 取り出し部
- 305 超流通ヘッダ復号化部
- 306 超流通コンテンツ復号化部
- 307 固有情報取り出し部
- 308 超流通コンテンツ再暗号化部
- 309 記録部
- 310 課金部
- 312 課金情報格納部
- 313 通信部
- 314 記録回数管理部
- 400 デジタルデータ再生装置
- 401 再生部
- 402 再生回数管理部
- 500 通信回線
- 600 ホストコンピュータ
- 650 買取用途の記録媒体
- 700 コンテンツパッケージング装置
- 706 コンテンツ符号化部

(23) 00-196585 (P2000-196585A)

- 707

コンテンツ品質 暗号対応表格納部
- 708

コンテンツ暗号化部
- 709

コンテンツ梱包部
- 710

販売用コンテンツ
- 711

試供用コンテンツ
- 801~809

コンテンツ再生装置
- 810

ハードウェア性能 復号対応表格納部
- 811

ハードウェア性能評価部
- 812

コンテンツ開梱部
- 813

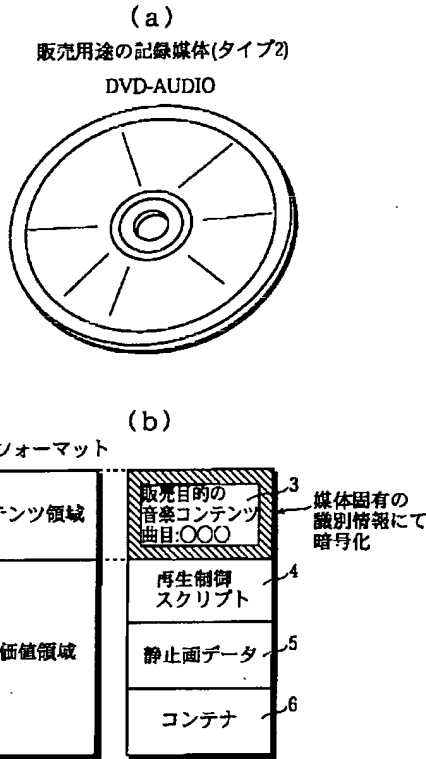
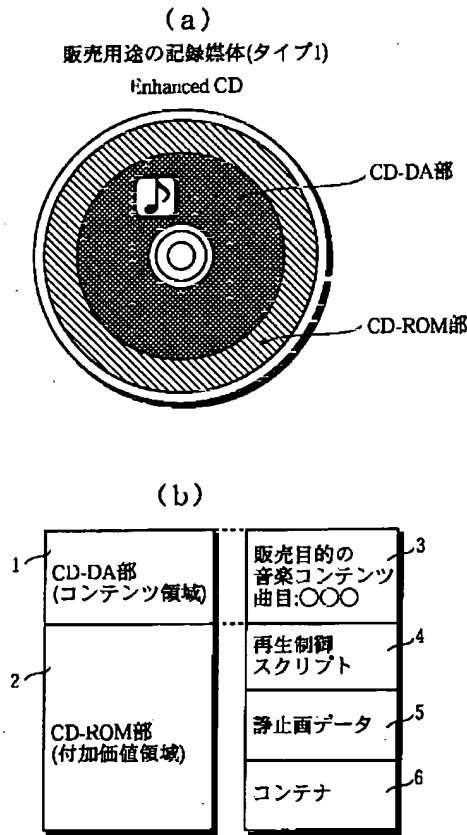
コンテンツ復号化部
- 814

コンテンツ格納部
- 815

コンテンツ再生部

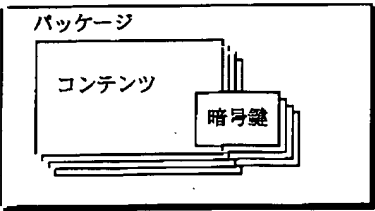
【図1】

【図2】



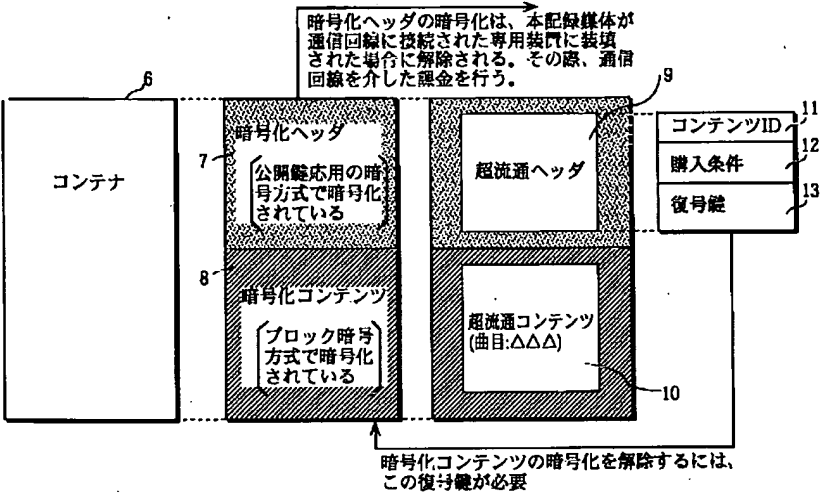
【図3】

【図18】



(24) 00-196585 (P2000-196585A)

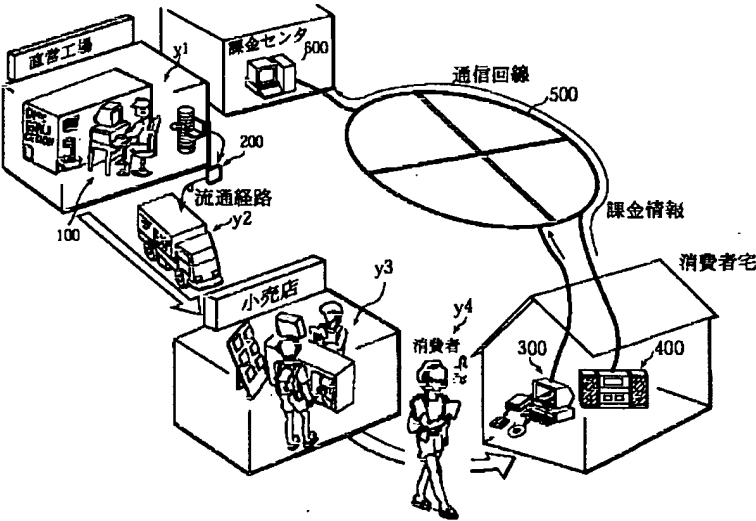
【図4】



【図5】

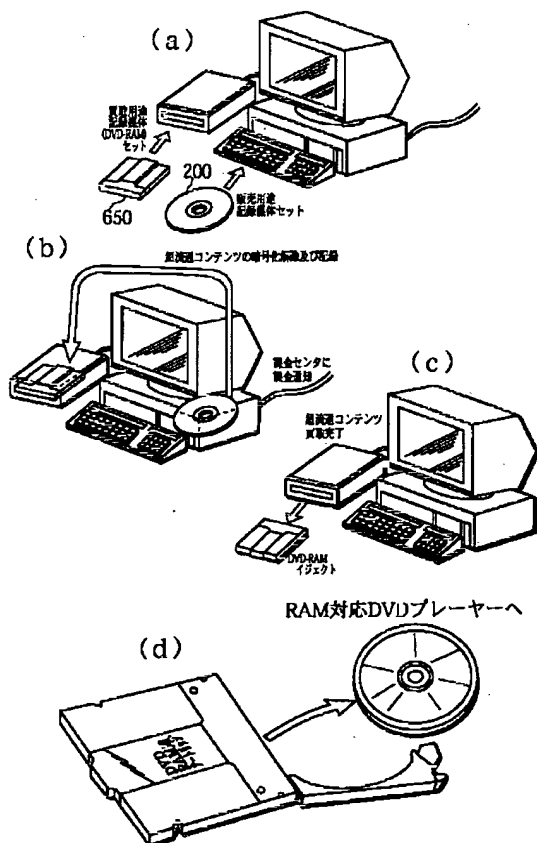
名称	内容
再生許可回数	再生可能な回数を記述
デジタル出力許可回数	デジタル出力を許可するか否か。許可する場合はその回数を記述
再生許可時間	再生可能な時間を記述
再生許可期日	再生可能な期日を記述
課金情報	買取時の価格や再生回数による使用料金を記述

【図6】

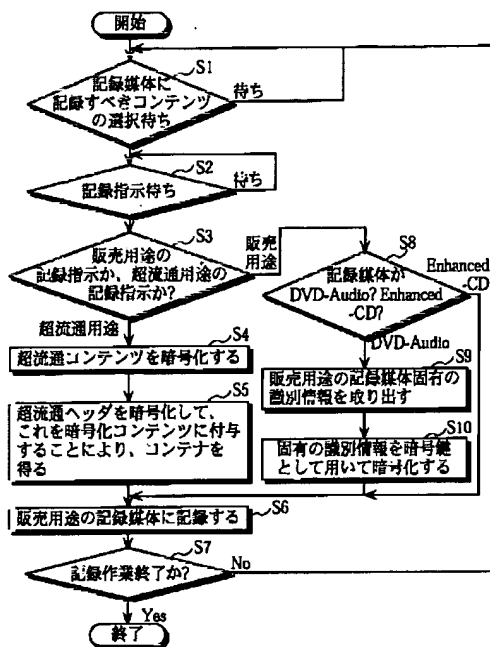


(25) 00-196585 (P2000-196585A)

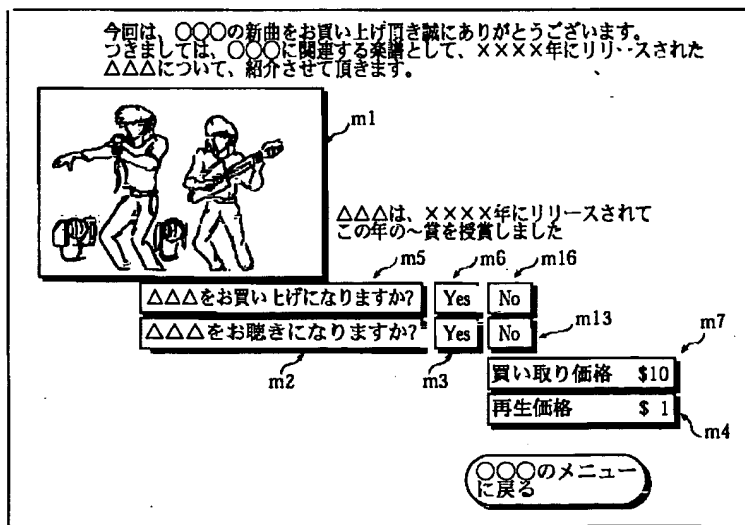
【図7】



【図10】

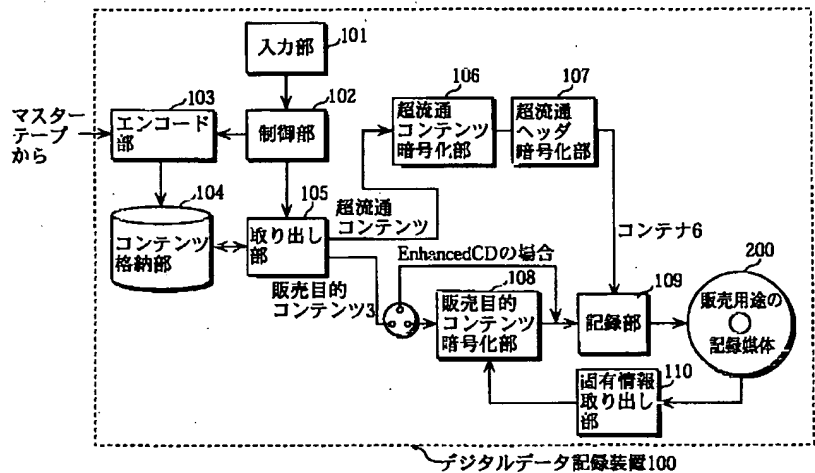


【図8】

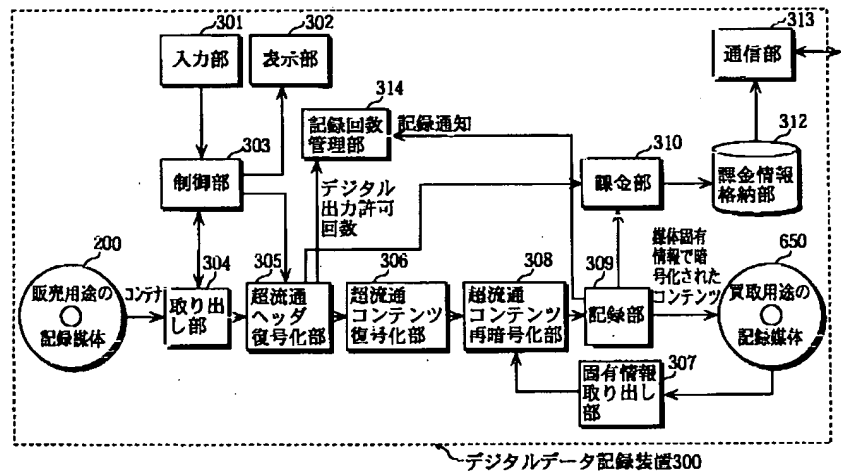


(26) 00-196585 (P2000-196585A)

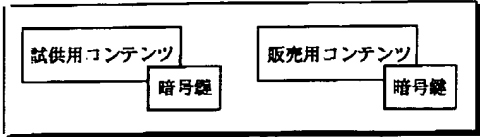
【図9】



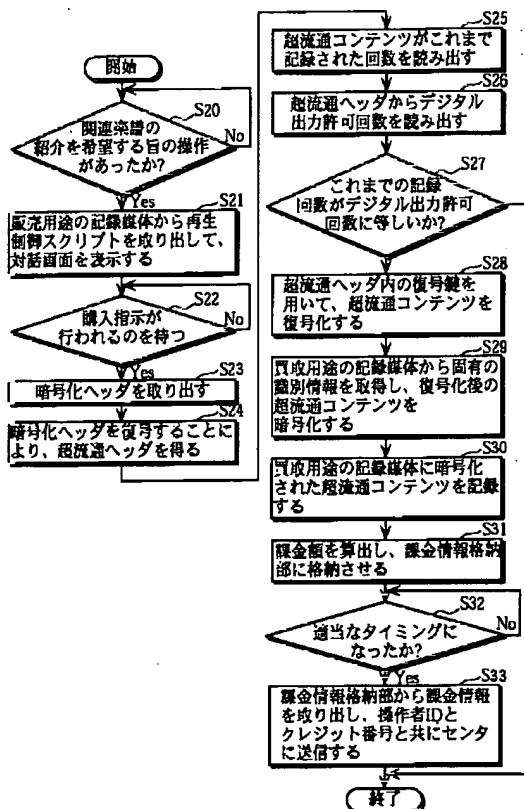
【図11】



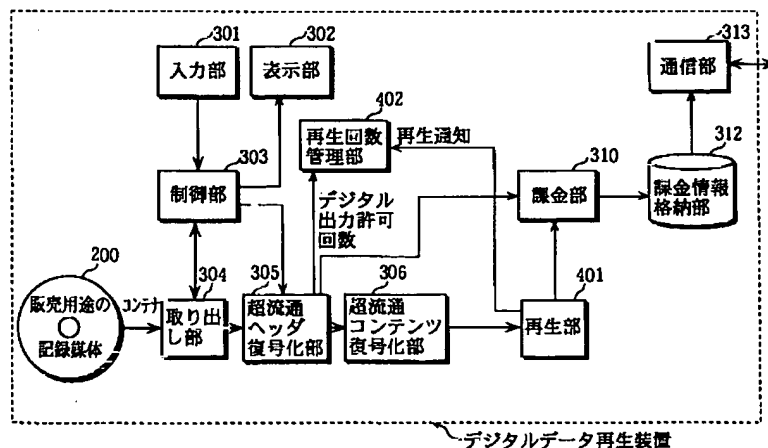
【図20】



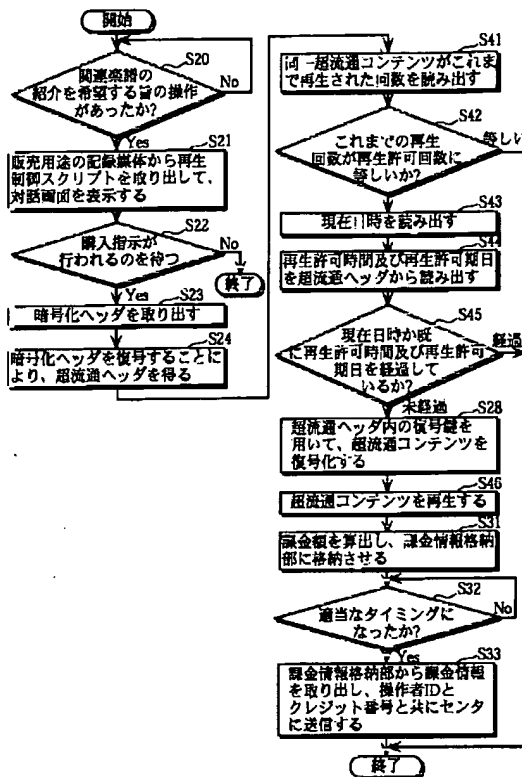
【图12】



【图 13】

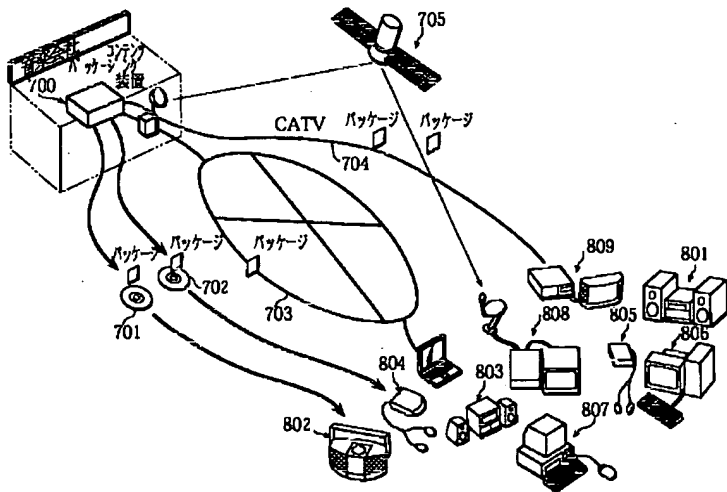


【図14】

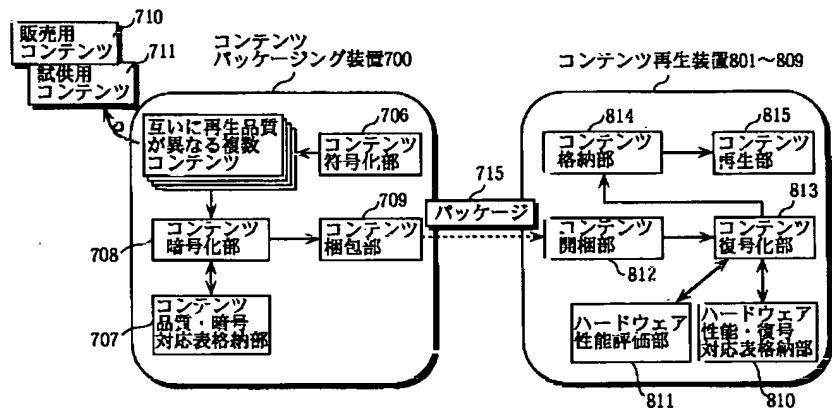


(28) 00-196585 (P2000-196585A)

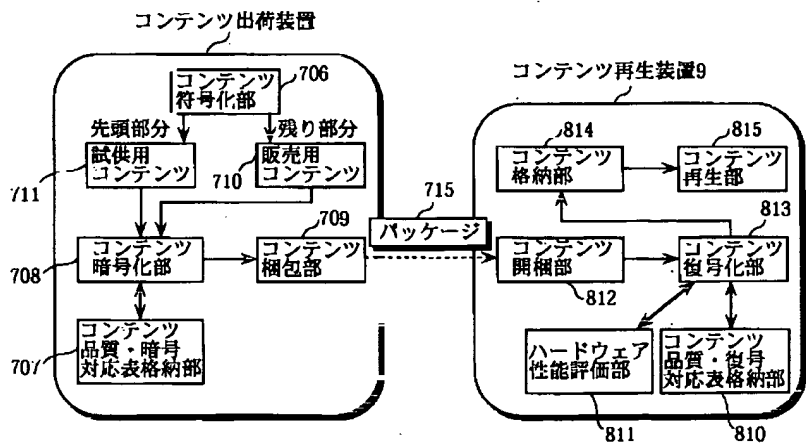
【図15】



【図16】



【図19】



(29) 00-196585 (P2000-196585A)

【図17】

(a)

コンテンツレベル	量子化ビット数	サンプリング周波数
ランク1	24 bit	96 KHz
ランク2	16 bit	44.1 KHz
ランク3	16 bit	22.05 KHz

(b)

コンテンツレベル	暗号鍵	暗号アルゴリズム
ランク1	1024 bit	RSA
ランク2	512 bit	RSA
ランク3	56 bit	DES

(c)

ハードウェア性能レベル	復号鍵	復号アルゴリズム
ランクA	1024 bit	RSA
ランクB	512 bit	RSA
ランクC	56 bit	DES

フロントページの続き

(72)発明者 小塚 雅之
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
(72)発明者 青山 昇一
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 徳田 克己
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
(72)発明者 平田 昇
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

【発明の名称】

コンテンツを記録した記録媒体、デジタルデータ記録装置、デジタルデータ再生装置、パッケー
ジを作成するコンテンツパッケージング装置、コンテンツ再生装置、コンピュータ読み取り可能
な記録媒体、記録方法、再生方法、パッケージング方法、コンテンツパッケージング装置と、コ
ンテンツ再生装置とからなるシステム